

Kaspersky Anti Targeted Attack Platform

Administrator's Guide

Application version: 3.6

Dear User,

Thank you for trusting us with your security. We hope that this document will help you in your work and will provide answers regarding this software product.

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky Lab): 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 Lab.

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

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

Kaspersky Lab 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 damages associated with the use of such documents.

Document revision date: 5/21/2019

© 2019 AO Kaspersky Lab. All Rights Reserved.

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

Table of Contents

Document conventions	17
Kaspersky Anti Targeted Attack Platform	18
What's new	20
About Kaspersky Threat Intelligence Portal	21
Distribution kit	21
Hardware and software requirements	22
Requirements for the Endpoint Sensors component	22
Compatibility of the Endpoint Sensors component with other programs.....	23
Requirements for the Central Node component.....	29
Requirements for the Sensor component.....	29
Requirements for the Sandbox component.....	30
Common scenarios for deployment and installation of program components	30
Two-server deployment scenario	33
Three-server deployment scenario.....	34
Scenario of deployment on four or more servers.	35
Scenario for deploying KEDR functionality without a Sandbox component.....	35
Scenario for deploying KEDR functionality with a Sandbox component.....	37
Program architecture	38
Sensor component.....	38
Central Node component.....	39
Sandbox component.....	39
Endpoint Sensors component	40
Operation of the program.....	41
Distributed solution and multitenancy mode	43
Distributed mode and multitenancy transition scenario.....	45
Modifications of program settings for distributed solution mode and multitenancy	45
Assigning the PCN role to a server	49
Assigning the SCN role to a server	50
Processing SCN to PCN connection requests	50
Viewing information about organizations, PCN and SCN servers	51
Adding an organization to the PCN server	52
Removing an organization from the PCN server	52
Renaming an organization on the PCN server	53
Disconnecting an SCN from PCN.....	53
Modifications of program settings for disconnecting an SCN from PCN.....	54
Decommissioning an SCN server.....	57

About data provision	58
Data of the Central Node and Sensor components	59
Data in logs and trace files	59
Data in alerts	62
Data in events	65
Targeted Attack Analyzer data	67
Data in reports	68
Data on objects in Backup	69
Data on program settings	69
Endpoint Sensors component data	76
Data received from the Central Node component	77
Data in logs and trace files	78
Data in alerts and events	80
Data contained in task completion reports	81
Data contained in an install log	82
Data on files that are blocked from starting	82
Data related to the performance of tasks	82
Data contained in dump files	83
Sandbox component data	85
Data transmitted between program components	86
Program licensing	91
About the End User License Agreement	91
About the license	91
About the license certificate	92
About the key	92
About the key file	92
Viewing information about the license and added keys	93
Viewing the text of the End User License Agreement in the web interface of the Central Node	93
Viewing the text of the Privacy Policy in the web interface of the Central Node	94
Viewing information about the third-party code used in the program	94
Viewing the text of the End User License Agreement in the web interface of the Sandbox	94
Viewing the text of the End User License Agreement on the computer with the Endpoint Sensors component	95
Adding a key	95
Replacing a key	95
Removing a key	96
Program modes based on the license	96
Installing and performing initial configuration of the program	97
Preparing for installing program components	97
Preparing the IT infrastructure for program components installation	97
Preparing the IT infrastructure for integration with a mail server used for receiving messages via POP3	99

Preparing the IT infrastructure for integration with a mail server used for receiving messages via SMTP	100
Preparing the virtual machine for installing the Sandbox component	100
Procedure for installing and configuring program components	101
Installing the Sandbox component	101
Step 1. Viewing the End User License Agreement and Privacy Policy	101
Step 2. Selecting a disk for installing the Sandbox component	102
Step 3. Creating the Sandbox administrator account	102
Step 4. Selecting the controlling network interface in the list	103
Step 5. Assigning the address and network mask of the controlling interface	103
Step 6. Configuring a static network route	103
Installing and configuring the Central Node and Sensor components on the same server	105
Step 1. Starting installation of the Central Node and Sensor components and selecting a server role	105
Step 2. Viewing the End User License Agreement and Privacy Policy	106
Step 3. Selecting a disk for installing the Central Node and Sensor components	106
Step 4. Creating an account for working in the administrator menu and in the server management console	107
Step 5. Assigning the host name	107
Step 6. Enabling a network interface for the first time	107
Step 7. Configuring the default network route	108
Configuring the network route using a DHCP server	108
Configuring a static network route	108
Step 8. Configuring DNS settings	109
Assigning DNS addresses using a DHCP server	109
Assigning static DNS addresses	109
Step 9. Configuring proxy server connection settings	110
Enabling and disabling the use of a proxy server	110
Configuring proxy server connection settings	110
Enabling and disabling the use of a proxy server when connecting to local addresses	111
Step 10. Setting the time zone	111
Step 11. Configuring time synchronization with an NTP server	111
Step 12. Connecting to the server with the Sandbox component	112
Step 13. Allocating the disk for the Targeted Attack Analyzer component's database	113
Step 14. Creating a local administrator account for the web interface	113
Step 15. Configuring receipt of mirrored traffic from SPAN ports	114
Step 16. Configuring integration with a proxy server via ICAP	114
Step 17. Configuring integration with a mail server via POP3	115
Step 18. Configuring integration with a mail server via SMTP	117
Installing and configuring the Sensor component on a separate server	119
Step 1. Starting installation of the Sensor component and selecting a server role	119
Step 2. Viewing the End User License Agreement and Privacy Policy	120
Step 3. Selecting a disk for installing the Sensor component	120

Step 4. Creating an account for working in the administrator menu and in the server management console	121
Step 5. Assigning the host name.....	121
Step 6. Enabling a network interface for the first time.....	121
Step 7. Configuring the default network route	122
Configuring the network route using a DHCP server	122
Configuring a static network route.....	122
Step 8. Configuring DNS settings.....	123
Assigning DNS addresses using a DHCP server.....	123
Assigning static DNS addresses	123
Step 9. Configuring proxy server connection settings	124
Enabling and disabling the use of a proxy server	124
Configuring proxy server connection settings	124
Enabling and disabling the use of a proxy server when connecting to local addresses	125
Step 10. Setting the time zone	125
Step 11. Configuring time synchronization with an NTP server	126
Step 12. Connecting to the server with the Central Node component	126
Step 13. Selecting the Central Node server as the source of Sensor component database updates	127
Step 14. Configuring receipt of mirrored traffic from SPAN ports	127
Step 15. Configuring integration with a proxy server via ICAP	128
Step 16. Configuring integration with a mail server via POP3	128
Step 17. Configuring integration with a mail server via SMTP	130
Installing and removing the Endpoint Sensors component	132
Special considerations for installing the Endpoint Sensors component if the program is used together with KES	132
Installing the Endpoint Sensors component	133
Preparing an SSL connection for data exchange between the Endpoint Sensors and Central Node components.....	134
Downloading an SSL certificate from the server with the Central Node component	134
Creating an SSL certificate on the server with the Central Node component.....	135
Uploading an independently prepared SSL certificate to the server with the Central Node component.....	135
Preparing and uploading an SSL certificate to Active Directory	137
Removing the Endpoint Sensors component	139
Configuring traffic redirection from the Endpoint Sensors components to the Sensor component.....	140
Enabling and disabling traffic redirection from the Endpoint Sensors components	140
Authorizing the Sensor component on a server with the Central Node component	141
Managing Endpoint Sensors components in Kaspersky Security Center	142
Creating an Endpoint Sensors installation package.....	142
Remotely installing the Endpoint Sensors component.....	144
Remotely changing the settings of the Endpoint Sensors component.....	145
Remotely uninstalling the Endpoint Sensors component.....	147

Remotely starting and stopping the Endpoint Sensors component	147
Creating a policy for remote management of the Endpoint Sensors component.....	148
Reconfiguring a policy for remote management of the Endpoint Sensors component.....	149
Receiving data from the Endpoint Sensors component in the Kaspersky Security Center Administration Console	150
Creating a selection of computers based on the presence or properties of Endpoint Sensors components	150
Receiving data on the status of the Endpoint Sensors component on a specific computer	153
Getting started with the program	154
Getting started with the program web interface.....	154
Getting started with the program administrator menu	154
Getting started with the program in Technical Support Mode	155
Managing accounts of program administrators and users.....	156
Creating an administrator account for the program web interface	158
Creating a user account for the program web interface	159
Changing access rights of a program web interface user account	160
Enabling and disabling an administrator account or user account of the program web interface	161
Changing the password of a program administrator or user account	161
Changing the password of your account	162
Participation in Kaspersky Security Network and use of Kaspersky Private Security Network.....	163
Viewing the KSN Statement and configuring participation in KSN.....	164
Enabling the use of KPSN	164
Configuring a connection to a local reputation database of KPSN	164
Configuring information to be saved to a local reputation database of KPSN	165
Declining participation in KSN and use of KPSN	165
Managing the Sandbox component through the web interface	166
Updating the Sandbox component databases	166
Updating databases manually	166
Selecting a database update source	167
Enabling and disabling a proxy server for database update	167
Configuring proxy server connection settings for database update	167
Configuring connection between the Sandbox and Central Node components.....	168
Creating a request for connection to Sandbox in the Central Node administrator menu.....	168
Processing connection requests from the Central Node servers in the Sandbox web interface	169
Configuring the Sandbox component network interfaces.....	170
Configuring DNS settings	170
Configuring settings of the management network interface	170
Configuring settings of a network interface used for Internet access of processed objects	171
Adding, changing and removing static network routes.....	171
Updating the Sandbox system.....	172
Setting the Sandbox system date and time	173

Installing and configuring images of operating systems and software required for the operation of the Sandbox component.....	173
Downloading ISO images of operating systems and software required for the operation of the Sandbox component	174
Creating virtual machines with images of operating systems and software required for the operation of the Sandbox component	174
Installing virtual machines with images of operating systems and software required for the operation of the Sandbox component	175
Deleting all pending virtual machines	175
Setting the maximum number of simultaneously running virtual machines	176
Downloading the Sandbox system log to the hard drive	176
Exporting the Sandbox parameters	176
Importing the Sandbox parameters	177
Restarting the Sandbox server	178
Shutdown of the Sandbox server	178
Changing the Sandbox administrator account password	178
For an administrator: Getting started with the program web interface	179
Kaspersky Anti Targeted Attack Platform Interface.....	179
Monitoring program operation	180
About widgets and layouts.....	180
Selecting an organization and a server to manage in the Dashboard section	181
Adding a widget to the current layout	181
Moving a widget in the current layout.....	181
Removing a widget from the current layout.....	182
Saving a layout to PDF	182
Configuring the period for displaying data in widgets.....	182
Monitoring the receipt and processing of incoming data	183
Monitoring the queues for data processing by program modules and components	184
Monitoring the processing of data by the Sandbox component	185
Viewing information about failures of program modules and components	185
Managing Central Node, PCN, or SCN servers using the program web interface.....	187
Configuring the date and time on the server	187
Powering off and restarting the server	188
Replacing the server certificate	188
Saving a server certificate file on a computer	189
Assigning a server DNS name	189
Configuring DNS settings	190
Enabling and disabling the network interface.....	190
Configuring settings of the network interface	191
Configuring the default network route	191
Configuring proxy server connection settings	192
Managing the Sensor component.....	193

Processing a connection request from the Sensor component.....	193
Viewing the table of servers with the Sensor component	193
Configuring the maximum size of a scanned file	194
Configuring receipt of mirrored traffic from SPAN ports	194
Configuring integration with a mail server via SMTP	195
Configuring TLS encryption of connections with a mail server via SMTP	196
Enabling integration with a proxy server via ICAP	197
Configuring integration with a mail server via POP3	198
Managing the Endpoint Sensors component.....	199
Selecting an organization to manage in the Endpoint Sensors section	199
Viewing the Endpoint Sensors table on a standalone Central Node server	200
Viewing the Endpoint Sensors table on a standalone Central Node server with KSC integration.....	200
Viewing the Endpoint Sensors table in distributed solution and multitenancy mode	202
Viewing information about a host	203
Filtering and searching Endpoint Sensors by host name	203
Filtering and searching Endpoint Sensors that have been isolated from the network	204
Filtering and searching Endpoint Sensors by PCN and SCN server names	205
Filtering and searching Endpoint Sensors by computer IP address	205
Filtering and searching Endpoint Sensors by operating system version on the computer	206
Filtering and searching Endpoint Sensors based on the Endpoint Sensor component version	207
Filtering and searching Endpoint Sensors based on their activity.....	207
Quickly creating a filter for computers with the Endpoint Sensors component	208
Clearing the Endpoint Sensors filter	209
Configuring Endpoint Sensors activity indicators	209
Creating a task for restarting the Endpoint Sensors components in KSC	210
Configuring integration with the Sandbox component.....	211
Viewing the table of servers with the Sandbox component.....	211
Creating a request to connect to the server with the Sandbox component	211
Enabling and disabling a connection with the Sandbox component	212
Deleting a connection with the Sandbox component	212
Configuring integration with external systems	213
Viewing the table of external systems	213
Processing a request from an external system	214
Removing an external system from the list of those allowed to integrate	214
Configuring the priority for processing traffic from mail sensors	214
Configuring integration with an SIEM system.....	215
Enabling and disabling event logging to a local log	215
Enabling and disabling event logging to a remote log.....	215
Configuring the main settings for SIEM system integration	215
Enabling and disabling TLS encryption of the connection with the SIEM system.....	216
Loading a TLS certificate.....	216

Content and properties of syslog messages about alerts	216
Configuring integration with Kaspersky Security Center	225
Enabling and disabling integration with Kaspersky Security Center	225
Configuring the settings for integration with Kaspersky Security Center	226
Configuring server settings for delivery of notifications	226
About database updates	227
Selecting a database update source	227
Updating databases manually	227
Creating a list of passwords for archives	228
For a security officer: Getting started with the program web interface	229
Kaspersky Anti Targeted Attack Platform Interface	229
Selecting an organization to manage in the web interface of the program	230
Monitoring program operation	231
About widgets and layouts	231
Adding a widget to the current layout	232
Moving a widget in the current layout	232
Removing a widget from the current layout	232
Saving a layout to PDF	233
Configuring the period for displaying data in widgets	233
Configuring the widget display size	234
Main principles of working with "Alerts" widgets	234
Table of alerts	236
Filtering and searching alerts	239
Filtering alerts by VIP status	239
Filtering and searching alerts by time	239
Filtering alerts by level of importance	240
Filtering and searching alerts by categories of objects detected	240
Filtering and searching alerts by obtained information	241
Filtering and searching alerts by source address	242
Filtering and searching alerts by destination address	242
Filtering and searching alerts by server name	243
Filtering and searching alerts based on names of program modules and components	243
Filtering and searching alerts by the status of their processing by the user	245
Quickly creating an alert filter	245
Clearing an alert filter	246
Viewing alerts	247
Viewing information about an alert	248
General information about an alert	248
Information in the Object information section	248
Information in the Alert information section	249
Information in the Scan results section	250

Information in the Network event section	251
Information in the Sandbox scan results section	251
Information in the Remote hosts section	252
Information in the Hosts section	253
Information about network activity of the computer in the Processes section	253
Information in the User account details section	254
Information in the Modules loaded into the process section	254
Information in the Change log section	255
Sending alert data	255
User actions performed on alerts	257
Assigning several alerts to a specific user	257
Assigning alerts to yourself or to another user	257
Marking the completion of single alert processing	258
Marking the completion of alerts processing	258
Modifying the status of VIP alerts	259
Adding a comment to an alert	259
Events database threat hunting	260
Searching events using design mode	260
Searching events using source code mode	262
Changing the event search conditions	263
Uploading an IOC file and searching for events based on conditions defined in the IOC file	264
Creating an IOA rule based on event search conditions	265
Event information	266
Viewing the table of events	266
Viewing information about an event	267
Information about process startup	268
Information about module loading	269
Information about a remote connection	269
Information about prevention rule triggering	270
Information about document blocking	271
Information about file creation	271
Information about an event in the Windows log	272
Information about changes in the registry	272
Information about port listening	273
Information about driver loading	273
Information about changing a host name	274
Information about the alert	274
Information about alert processing results	275
Managing the Endpoint Sensors component	277
Viewing the Endpoint Sensors table on a standalone Central Node server	277
Viewing the Endpoint Sensors table on a standalone Central Node server with KSC integration	278

Viewing the Endpoint Sensors table in distributed solution and multitenancy mode	280
Viewing information about a host	280
Filtering and searching Endpoint Sensors by host name	282
Filtering and searching Endpoint Sensors that have been isolated from the network	282
Filtering and searching Endpoint Sensors by PCN and SCN server names	283
Filtering and searching Endpoint Sensors by computer IP address	284
Filtering and searching Endpoint Sensors by operating system version on the computer	284
Filtering and searching Endpoint Sensors based on the Endpoint Sensor component version	285
Filtering and searching Endpoint Sensors based on their activity	286
Filtering and searching Endpoint Sensors by operating errors of the component	286
Quickly creating a filter for computers with the Endpoint Sensors component	287
Clearing the Endpoint Sensors filter	288
Configuring Endpoint Sensors activity indicators	288
Supported interpreters and processes	288
Network isolation of hosts with the Endpoint Sensors component	291
Creating a network isolation rule	291
Adding an exclusion from a network isolation rule	292
Disabling a network isolation rule	292
Managing tasks	294
Viewing the task table	294
Viewing information about a task	295
Creating a process termination task	296
Creating a program execution task	297
Creating a file download task	298
Creating a file deletion task	299
Creating a file quarantine task	300
Creating a quarantined file recovery task	301
Creating a copy of a task	301
Deleting a task	302
Filtering tasks by creation time	302
Filtering tasks by type	303
Filtering tasks by name	303
Filtering tasks by file name and path	304
Filtering tasks by description	304
Filtering tasks by server name	305
Filtering tasks based on the name of the user that created the task	305
Filtering tasks by processing status	306
Clearing a task filter	306
Managing policies (prevention rules)	307
Viewing the prevention rule table	307
Viewing a prevention rule	308

Creating a prevention rule	309
Enabling and disabling a prevention	310
Deleting a prevention rule.....	310
Filtering preventions by name	310
Filtering prevention rules by type.....	311
Filtering preventions by file hash	311
Filtering preventions by server name	312
Clearing a prevention rule filter.....	312
Managing indicators of compromise and attack	314
IOC scan of events	314
Viewing the table of IOC files	315
Viewing information about an IOC file	316
Uploading an IOC file	316
Downloading an IOC file to a computer	317
Enabling and disabling the automatic use of an IOC file when scanning events.....	317
Deleting an IOC file	318
Searching IOC scan results.....	318
Filtering and searching IOC files	318
Clearing an IOC file filter	319
Configuring an IOC scan schedule.....	319
Supported OpenIOC Indicators of Compromise	319
IOA analysis of events	325
Viewing the IOA rule table	326
Viewing information about an IOA rule.....	326
Enabling or disabling an IOA rule	327
Adding an IOA rule	328
Editing an IOA rule	329
Deleting an IOA rule	329
Viewing an IOA white list	330
Viewing information about an IOA rule in the white list	331
Adding an IOA rule to the white list	331
Removing an IOA rule from the white list.....	332
Viewing the IOA analysis results	333
Filtering and searching IOA rules	334
Clearing an IOA rules filter	334
Managing objects in Backup.....	335
Viewing the table of objects that were placed in Backup	336
Viewing information about an object in Backup.....	336
Downloading objects from Backup	337
Uploading objects to Backup	338
Scanning objects from Backup.....	338

Deleting objects from Backup	338
Filtering objects in Backup by object type	339
Filtering objects in Backup by object description	339
Filtering objects in Backup based on scan results	340
Filtering objects in Backup based on the name of Central Node, PCN, or SCN server	340
Filtering objects in Backup by object source	341
Filtering objects based on the time they were placed in Backup	341
Clearing a Backup objects filter	342
Viewing space usage in Backup and Quarantine	342
Managing reports	343
Creating a template	343
Creating a report based on a template	345
Viewing the table of templates and reports	345
Viewing a report	346
Downloading a report to a local computer	346
Editing a template	346
Filtering templates by name	347
Filtering templates based on the name of the user that created the template	348
Filtering templates by creation time	348
Clearing a template filter	349
Deleting a template	349
Filtering reports by creation time	349
Filtering reports by name	350
Filtering reports by the name of the server with the Central Node component	350
Filtering reports based on the name of the user that created the report	350
Clearing a report filter	351
Deleting a report	351
Sending notifications	352
Viewing the table of rules for sending notifications	352
Creating a rule for sending notifications about alerts	352
Creating a rule for sending notifications about the operation of program components	353
Enabling and disabling a rule for sending notifications	353
Modifying a rule for sending notifications	354
Deleting a rule for sending notifications	354
Filtering and searching notification forwarding rules by rule type	354
Filtering and searching notification forwarding rules based on the notification subject	355
Filtering and searching notification forwarding rules by email address	355
Filtering and searching notification forwarding rules based on their status	355
Clearing a notification forwarding rule filter	356
Managing rules for assigning the VIP status to alerts	357
Adding a VIP status assignment rule	357

Deleting a VIP status assignment rule	357
Modifying a VIP status assignment rule	358
Importing a list of VIP status assignment rules	358
Exporting a list of VIP status assignment rules	358
Filtering and searching by type of VIP status assignment rule	359
Filtering and searching by value of VIP status assignment rule	359
Filtering and searching by description of VIP status assignment rule	359
Clearing a VIP status assignment rule filter	360
Managing YARA rules	360
Uploading YARA rules	360
Updating YARA rules	361
Deleting YARA rules	361
Managing a white list	362
Adding a record to the white list	362
Removing a record from the white list	363
Modifying a record in the white list	364
Importing a white list	364
Exporting a white list	364
Filtering and searching records in the white list based on the type of rule	365
Filtering and searching records in the white list based on a value of rules	365
Clearing a white list record filter	366
Creating a list of passwords for archives	366
Creating a backup copy and restoring the program from backup	367
Creating a backup copy of the program from the program administrator menu	369
Downloading a file containing a backup copy of the program from the Central Node or PCN server to the hard drive of the computer	369
Uploading a file containing a backup copy of the program from your computer to the Central Node server	370
Restoring the program from a backup copy through the program administrator menu	370
Creating a backup copy of the program in Technical Support Mode	371
Restoring the program from a backup copy in Technical Support Mode	372
Upgrading Kaspersky Anti Targeted Attack Platform	373
Upgrading the program from version 3.5 to version 3.6	375
Installing program update packages	377
Interaction with external systems via API	379
Interaction between an external system and Kaspersky Anti Targeted Attack Platform	379
Creating a request to integrate an external system with Kaspersky Anti Targeted Attack Platform	379
API for scanning objects of external systems	380
Scanning objects	380
Viewing scan results	381
Deleting scan results	382
Viewing filters	383

API for sending alert information to external systems	384
Requesting alert information.....	384
Scope of transmitted data.....	385
Data on detected objects.....	386
Data on detected threats	389
Data on the environment of detected objects.....	391
Contacting the Technical Support Service	395
How to obtain Technical Support.....	395
Technical support by phone	395
Technical Support via Kaspersky CompanyAccount.....	395
Sources of information about the program	396
Glossary	397
AO Kaspersky Lab	404
Information about third-party code.....	405
Trademark notices	406

Document conventions

This document uses the following conventions (see table below).

Table 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and boxed. Warnings show information about actions that may have unwanted consequences.
We recommend that you use...	Notes are boxed. Notes provide additional and reference information.
Example: ...	Examples are given on a blue background under the heading "Example".
<i>Update</i> means... The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: <ul style="list-style-type: none"> • New terms • Names of program statuses and events
Press ENTER . Press ALT+F4 .	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. These keys have to be pressed simultaneously.
Click the Enable button.	Names of program interface elements, such as entry fields, menu items, and buttons, are set off in bold.
► <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, type <code>help</code> . The following message then appears: <code>Specify the date in dd:mm:yy format.</code>	The following types of text content are set off with a special font: <ul style="list-style-type: none"> • Text in the command line. • Text of messages that the program displays on screen. • Data to be entered using the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of a variable, the corresponding value should be inserted, with angle brackets omitted.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform (hereinafter also referred to as "the program") is a solution designed for the protection of a corporate IT infrastructure and timely detection of threats such as *zero-day attacks*, *targeted attacks*, and complex targeted attacks known as *advanced persistent threats* (hereinafter also referred to as "APT"). The program is developed for corporate users.

Kaspersky Anti Targeted Attack Platform includes two functional blocks:

- Kaspersky Anti Targeted Attack (hereinafter also referred to as "KATA"), which provides perimeter security for the enterprise IT infrastructure.
- Kaspersky Endpoint Detection and Response (hereinafter also referred to as "KEDR"), which provides protection for the local area network of the organization.

KEDR is licensed separately from KATA. To activate this functionality, you need to use a separate key. You can purchase KEDR with KATA or separately.

The program can receive and process data in the following ways:

- *Integrate into the local area network, receive and process mirrored SPAN, ERSPAN and RSPAN traffic*, and extract objects and metadata from the HTTP, FTP, SMTP, and DNS protocols.
- Connect to the proxy server via the ICAP protocol, receive and process data of HTTP and FTP traffic, as well as HTTPS traffic if the administrator has configured SSL certificate replacement on the proxy server.
- Connect to the mail server via the POP3 (S) and SMTP protocols, receive and process copies of e-mail messages.
- Integrate with the Kaspersky Lab applications Kaspersky Secure Mail Gateway and Kaspersky Security for Linux® Mail Server, receive, and process copies of email messages.

For detailed information on Kaspersky Secure Mail Gateway and Kaspersky Security for Linux Mail Server, please refer to the documentation on these applications.

- Integrate with external systems with the use of the REST API interface and scan files on these systems.
- Receive data from individual computers that belong to the corporate IT infrastructure and run the Microsoft® Windows® operating system to constantly monitor processes running on those computers, active network connections, and files that are modified.
 - The Kaspersky Anti Targeted Attack Platform Endpoint Sensors component can be installed on individual computers and receive data from these computers.
 - Kaspersky Anti Targeted Attack Platform can be integrated with the Kaspersky Endpoint Security for Windows program by Kaspersky Lab (also referred to as "KES").

For details about Kaspersky Endpoint Security for Windows, see *Kaspersky Endpoint Security Help*.

The program uses the following means of Threat Intelligence:

- Infrastructure of Kaspersky Security Network (also referred to as "KSN") cloud services that provides access to the online Knowledge Base of Kaspersky Lab, which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

- Integration with the Kaspersky Private Security Network (KPSN) Kaspersky Lab application to access the reputation databases of Kaspersky Security Network and other statistical data without sending data from user computers to Kaspersky Security Network.
- Integration with the Kaspersky Lab information system known as Kaspersky Threat Intelligence Portal, which contains and displays information about the reputation of files and URLs.

The program can provide the user with the results of its performance and Threat Intelligence in the following ways:

- Display operation results on the Central Node PCN or SCN servers web interface.
- Publish alerts to a SIEM system already being used in your organization via the Syslog protocol.
- Integrate with external systems via the REST API and send information on detects to external systems on demand.
- Publish information on Sandbox component alerts in the local reputation database of Kaspersky Private Security Network.

Senior security officer and Security officer users can perform the following actions in the program:

- Monitor program performance.
- View the table of detected signs of targeted attacks and intrusions into the corporate IT infrastructure, filter and search alerts, and view and manage each alert.
- Look through the table of events occurring on the computers and servers of the organization IT infrastructure, search for threats, filter, view and work with each event.
- Run tasks on hosts with Endpoint Sensors component: start programs and stop processes, download and delete files, place objects and their copies in Backup and Quarantine, and restore them from Quarantine.
- Configure policies for preventing the startup of files that they consider to be unsafe on selected hosts with the Endpoint Sensors component.
- Isolate separate hosts with the Endpoint Sensors component from the network.
- Work with objects and their copies in Backup and Quarantine.
- Work with the OpenIOC standard files to search on signs of targeted attacks, infected and probably infected objects on hosts with the Endpoint Sensors component and in the Alerts database.
- Work with Indicators of Attack (IOA) to classify and analyze events.
- Manage reports on the program performance and on detects.
- Configure forwarding of notifications about alerts and about program operation problems to one or multiple email addresses.
- Manage a list of VIP group addresses and a white list of data, and add to the local reputation database of KPSN.

Local administrator and Administrator can use the program to:

- Configure program operation settings.
- Configure servers for the distributed solution and multitenancy mode of the program.
- Administer integration of the program with other programs and systems.
- Manage accounts of program users.
- Monitor program performance.

The program detects the following events occurring within the corporate IT infrastructure and notifies the user accordingly:

- A file has been downloaded or an attempt was made to download a file to a corporate LAN computer.
- A file has been sent to the email address of a user on the corporate LAN.
- A website link was opened on a corporate LAN computer.
- Network activity has occurred in which the IP address or domain name of a corporate LAN computer was detected.
- Processes have been started on a corporate LAN computer.

Kaspersky Anti Targeted Attack Platform evaluates events and advises the user to direct attention to each detected event (*alert*) according to the impact that this alert may have on computer or corporate LAN security based on Kaspersky Lab experience.

The Kaspersky Anti Targeted Attack Platform user independently makes a decision about further actions in response to alerts.

What's new

Kaspersky Anti Targeted Attack Platform now has the following new features:

- Multitenancy mode was implemented, enabling installation of Kaspersky Anti Targeted Attack Platform in distributed solution mode and its use to protect the infrastructure of multiple organizations. One or more Central Node servers can be used for the same organization. Each organization can manage the program independently from other organizations. The provider can manage data of several organizations.
- Targeted Attack Analyzer technology was improved: classification and automatic analysis of events and alerts added to check if they match indicators of attack (hereinafter also referred to as IOA) and the MITRE ATT&CK matrix. The IOA rule database is created by experts at Kaspersky Lab and is continuously updated. New events that triggered IOA rules are marked in the program interface. IOA rules contain descriptions of signs of attacks, examples and recommended countermeasures, links to the information on each sign of attacks in the MITRE ATT&CK knowledge base.
- Added classification of alerts by the Sandbox component in accordance with the MITRE ATT&CK matrix. The Sandbox component matches detected suspicious activities with attack phases, hacker techniques and methods in the MITRE ATT&CK matrix.
- Added the ability to create a custom database of indicators of attack (IOA) for classifying and analyzing events.
- Added a program deployment scenario which lets multiple Central Node servers connect to the same Sandbox servers.
- Added case sensitivity support for finding, editing, and deleting files, folders, and other objects in accordance with the standards of the NTFS file system.
- Implemented a new method for analyzing APK files of the Android™ operating system using a state-of-the-art cloud technology based on machine learning.
- Added monitoring of new registry keys — analyzing information on registry branches from the sections of HKEY_USERS/HKEY_CURRENT_USER.

- Expanded capabilities for cracking passwords of Microsoft Office documents and email messages. Implemented the ability to crack passwords of email attachments of the following formats: ArchiveRAR (RAR v5) and Archive7z (7z). Also added the ability to crack passwords of documents in PDF, Word, Excel®, and PowerPoint® formats. Passwords are looked up in an existing password database or derived from data in the email message body.
- Added sending of new Windows event types (Windows events logging) with the following IDs:
 - EventId 4776 – the computer attempted to verify user account data.
 - EventId 4648 – attempt to log in with credentials.
 - EventId 4768 – authentication ticket of the Kerberos service (TGT) was requested.
 - EventId 4769 – Kerberos service ticket was requested.

The update enables detection of the following attacks that use these Windows events:

- Pass-the-hash (4776, 4624).
- Keberoast (4769).
- Mimikatz (4624, 4648, 4768).
- Added support of API for sending information about Kaspersky Anti Targeted Attack Platform alerts to third-party solutions on request of the third-party solutions. The transmitted alert information can also contain additional information, for example triggered technologies, object types, alert importance.
- Optimized the performance of the program. Central Node and Sandbox servers now have 30% lower hardware requirements.

About Kaspersky Threat Intelligence Portal

For additional information about files that you consider to be suspicious, you can go to the website of the Kaspersky Lab application Kaspersky Threat Intelligence Portal, which analyzes each file for malicious code and shows information about the reputation of the file.

Access to the Kaspersky Threat Intelligence application is provided based on a fee. Authorization on the program website requires that a program access certificate is installed in the certificate storage on your computer. In addition, you must have a user name and password for accessing the program. For more details about the Kaspersky Threat Intelligence Portal, please visit the Kaspersky Lab website.

Distribution kit

The program distribution kit contains the following files:

1. Disk image (file with the iso extension) containing the installation files for the CentOS 7.4 operating system and for the Sensor and Central Node components.
2. Disk image (file with the iso extension) containing the installation files for the CentOS 6.9 operating system and for the Sandbox component.
3. Disk images (files with the iso extension) containing the Windows XP SP3, 64-bit Windows 7, and 64-bit Windows 10 operating systems on which the Sandbox component will run files.

4. Installation file for the Endpoint Sensors component (file with the msi extension).
5. End User License Agreement.
6. Privacy Policy.
7. KSN Statement.
8. File with information about third-party code used in Kaspersky Anti Targeted Attack Platform.

Hardware and software requirements

One of the following browsers must be installed on the computers in order to configure and work with the program over the web interface.

- Google Chrome™ for Windows version 74 or later.
- Google Chrome for Linux version 74 or later.
- Mozilla™ Firefox™ version 66 or later.
- Microsoft Edge 44 or later.
- Safari 12.0 or later.

Deploying the program on a virtual platform requires installing the VMware ESXi™ 5.5.0 or 6.7.0 hypervisor.

Requirements for the Endpoint Sensors component

The Endpoint Sensors component has predefined settings that determine the impact that the Endpoint Sensors component has on the performance of the local computer under scenarios of information retrieval and interaction with the Central Node component.

If Kaspersky Anti Targeted Attack Platform version 3.5 is installed on Central Node servers but Endpoint Sensors component version 3.0 is installed on computers of your organization's local area network, the following limitations on program operation are possible: IOC scan of files on computers with Endpoint Sensors version 3.0 and management of tasks and policies that were created on computers with Endpoint Sensors version 3.0 may be unavailable from Central Node servers.

Software requirements for installing the Endpoint Sensors component

One of the following operating systems:

- Windows 7 SP1 Enterprise x86 x64.
- Windows 8.1.1 Enterprise x86 x64.
- Windows 10 RS3 Enterprise x86 x64.
- Windows 10 RS4 Enterprise x86 x64.
- Windows 10 RS5 Enterprise x86 x64.
- Windows 10 RS6 Enterprise x86 x64.

- Windows Server® 2008 R2 Enterprise x64.
- Windows Server 2012 Standard x64.
- Windows Server 2012 R2 Standard x64.
- Windows Server 2016 Standard x64.

Kaspersky Endpoint Security including Endpoint Sensors component version 3.6 supports fewer operating systems than KES version 11.1.1 without a built-in Endpoint Sensors component.

If you are using the Endpoint Sensors component as part of Kaspersky Endpoint Security, please take into account the compatibility of program versions:

- The Endpoint Sensors component of Kaspersky Anti Targeted Attack Platform version 3.6 is included in KES version 11.1.1.
- The Endpoint Sensors component of Kaspersky Anti Targeted Attack Platform version 3.0 is included in KES version 10 SP2 MR3 and version 11.0.

Hardware requirements for installing the Endpoint Sensors components

Minimum configuration:

- CPU: 2 GHz or higher with SSE2 instruction set support.
- RAM: 2 GB.
- Disk subsystem: 2 GB of free space.
- One network adapter with a data transfer speed of 1 Gbit/s.

Recommended configuration:

- Intel® Core™ i3 Duo 3.10GHz or equivalent processor (with SSE2 support).
- RAM: 40 MB.
- Disk subsystem: 100 MB of free space.

When integrated with the Kaspersky Lab application Kaspersky Endpoint Security, Kaspersky Anti Targeted Attack Platform has limited functionality if the Windows Server 2008 SP2 x64 operating system is installed on the server hosting KES.

Compatibility of the Endpoint Sensors component with other programs

Kaspersky Anti Targeted Attack Platform does not support joint operation with programs not listed in this section.

Compatibility of the Endpoint Sensors component version 3.5 with Kaspersky Lab programs

You can use Kaspersky Endpoint Security for Windows version 10 SP2 MR3 or 11.0 and the standalone Endpoint Sensors component version 3.5 on the same computer. To do so:

1. Disable the Endpoint Sensors component in the KES program.

For more details on how to disable the Endpoint Sensors component in the KES program, refer to the *Kaspersky Endpoint Security Help* <https://help.kaspersky.com/KESWin/11.1.1/en-US/132664.htm>.

2. Install the standalone Endpoint Sensors component version 3.5 on all the computers of your organization's local area network on which you want to use the Endpoint Sensors component.

Compatibility of Endpoint Sensors component version 3.6 with Kaspersky Endpoint Security for Windows (KES)

Information about the compatibility of Endpoint Sensors component version 3.6 with the KES program is provided in the following table.

Kaspersky Endpoint Security version 11.1 is compatible only with the Endpoint Sensors component included with the KES program. You cannot install KES 11.1 and the standalone Endpoint Sensors component on the same computer.

Table 2. Compatibility of the Endpoint Sensors component with the KES program.

Version of the Kaspersky Lab program	Compatibility mode	Installing the standalone Endpoint Sensors component after installing the other program	Installing the other program after installing the standalone Endpoint Sensors component	Supported operating systems
<ul style="list-style-type: none"> KES10 SP1 MR3 KES10 SP1 MR4 	Joint operation.	Standard installation procedure.	Standard installation procedure.	
<ul style="list-style-type: none"> KSC 10 SP2 KSC 10 SP2 MR1 KSC 10 SP2 MR2 KSC 10 SP2 MR3 	Joint operation. Sending KES alert information (see page 274) is supported.	Standard installation procedure.	Standard installation procedure.	
<ul style="list-style-type: none"> KES 11.0.0 KES 11.0.1 KES 11.1 	The following scenarios are possible: <ul style="list-style-type: none"> Joint operation of KES and the standalone Endpoint Sensors component. Using the built-in Endpoint Sensors component as part of KES. 	To install the standalone Endpoint Sensors component, the Endpoint Sensors built in the KES program must be disabled. For more details on how to disable the Endpoint Sensors component in the KES program, refer to the <i>Kaspersky Endpoint Security Help</i> https://help.kaspersky.com/KESWin/11.1.1/en-US/132664.htm . If the component is not disabled, installation fails with an error.	Standard installation procedure.	

Version of the Kaspersky Lab program	Compatibility mode	Installing the standalone Endpoint Sensors component after installing the other program	Installing the other program after installing the standalone Endpoint Sensors component	Supported operating systems
KES 11.1.1	Only the built-in Endpoint Sensors component as part of KES is available. Joint operation of the standalone Endpoint Sensors component and KES is not supported.	Installation fails with an error. You can enable the built-in Endpoint Sensors component https://help.kaspersky.com/KESWin/11.1.1/en-US/132664.htm as part of the KES program.	KES removes the standalone Endpoint Sensors component.	<ul style="list-style-type: none"> • Windows 7 SP1 Enterprise x86 x64. • Windows 8.1.1 Enterprise x86 x64. • Windows 10 RS3 Enterprise x86 x64. • Windows 10 RS4 Enterprise x86 x64. • Windows 10 RS5 Enterprise x86 x64. • Windows 10 RS6 Enterprise x86 x64. • Windows Server 2008 R2 Enterprise x64. • Windows Server 2012 Standard x64. • Windows Server 2012 R2 Standard x64. • Windows Server 2016 Standard x64.

Compatibility of the Endpoint Sensors component version 3.6 with Kaspersky Security for Virtualization 5.1 Light Agent (KSV)

Installing the Endpoint Sensors component on the same virtual machine as the KSV program is supported for the following operating system:

- Windows Server 2008 R2 Enterprise x64
- Windows Server 2012 Standard x64
- Windows Server 2012 R2 Standard x64
- Windows Server 2016 Standard x64.

For KSV to run in the virtual infrastructure, one of the following hypervisors must be installed (depending on the virtualization platform):

- Microsoft Hyper-V® platform:
 - Microsoft Windows Server 2016 Hyper-V hypervisor (in full mode or in Server Core mode) with all available updates.
 - Microsoft Windows Server 2012 R2 Hyper-V hypervisor (in full mode or in Server Core mode) with all available updates.
- Citrix Hypervisor platform: Citrix XenServer 7.1 LTSR hypervisor.
- VMware vSphere™ platform:
 - VMware ESXi 6.7 hypervisor
 - VMware ESXi 6.5 hypervisor
 - VMware ESXi 6.0 hypervisor with the latest updates
- KVM (Kernel-based Virtual Machine) platform: KVM hypervisor with one of the following operating systems:
 - Ubuntu Server 18.04 LTS.
 - Ubuntu Server 16.04 LTS.
 - Red Hat Enterprise Linux® Server 7.5.
 - CentOS 7.5.
- Proxmox VE platform: Proxmox VE 5.2 hypervisor.
- Skala-R platform: R-Virtualization 7.0.6 hypervisor.
- HUAWEI FusionSphere platform: HUAWEI FusionCompute CNA 6.3.1 hypervisor.

Cloning virtual machines with installed Endpoint Sensors component and the KSV program is not supported. Clone the virtual machine, generate a new SMBIOS GUID for it, then install the Endpoint Sensors component.

Compatibility of the Endpoint Sensors component with third-party antivirus programs

One of the following third-party antivirus programs can be installed on computers on which you want to install the Endpoint Sensors component:

- Symantec™ Endpoint Protection.

- Trend Micro™ Maximum Security.
- Sophos Endpoint Protection.
- ESET NOD32 Business Edition Smart Security.
- BitDefender GravityZone Advanced Business Security.

If you install more than one third-party antivirus program, correct operation of the Endpoint Sensors component is not guaranteed.

If the RealTimes Desktop Service is installed on computers on which the Endpoint Sensors component will be installed, you are advised to uninstall it before installing the Endpoint Sensors component.

Requirements for the Central Node component

Hardware requirements for the server on which the Central Node component will be installed

The configuration of the server hosting the Central Node component depends on the volume of data processed by the program and the bandwidth of the communication channel.

Minimum hardware requirements for the server (communication channel bandwidth of 50 Mbit/s; 1,000 computers with the Endpoint Sensors component):

- CPU: 12 cores (24 threads), 2.7 GHz.
- RAM: 128 GB.
- Disk subsystem – two partitions: 2 TB of free space for the system partition and 4 TB of free space for storing the Targeted Attack Analyzer component's database.

It is recommended to use a disk array of RAID level 0, 5, 10 or an SSD disk.

- Two network adapters, each with a data transfer speed of 1 Gbit/s.

Requirements for the Sensor component

Hardware requirements for the server on which the Sensor component will be installed

The configuration of the server hosting the Sensor component depends on the volume of data processed by the program and the bandwidth of the communication channel.

Minimum hardware requirements for the server (communication channel bandwidth of 50 Mbit/s; the component processes mirrored traffic and email messages; processing time amounts to 120 messages per second):

- CPU: 16 cores, 2.7 GHz.
- RAM: 32 GB.
- Disk subsystem: 500 GB of free space.
- Two network adapters, each with a data transfer speed of 1 Gbit/s.

Requirements for the Sandbox component

Hardware requirements for the server on which the Sandbox component will be installed

The configuration of the server hosting the Sandbox component depends on the volume of data processed by the program, the number of simultaneously running virtual machines with images of operating systems, and the bandwidth of the communication channel.

Minimum hardware requirements for the server (communication channel bandwidth of 50 Mbit/s; 12 simultaneously running virtual machines; 3,500 files processed in 24 hours):

- Intel CPU with support for VT-x and EPT, 8 cores, 2.7 GHz.

AMD™ processors are not supported.

- RAM: 32 GB.
- Disk subsystem: 300 GB of free space.
- Two network adapters, each with a data transfer speed of 1 Gbit/s.

Calculate the number of simultaneously running virtual machines with images of operating systems as follows: multiply the number of processor cores by 1.5. Each virtual machine requires 1 GB of RAM.

Common scenarios for deployment and installation of program components

The scenario for deployment and installation of program components is determined by the planned load on the program servers.

The Endpoint Sensors component is installed on any computers that belong to the organization's IT infrastructure and run the Windows operating system. Outbound connections from computers with the Endpoint Sensors component to the server hosting the Central Node component must be allowed directly, without a proxy server.

You can install one or multiple Central Node components. If you install multiple Central Node components, you can use them independently of each other or combine them for centralized management in distributed solution (see page 43) mode.

The deployment scenario selection depends on the utilized program functionality (see page 96). All scenarios listed in this manual also apply to the deployment of the program on a virtual platform.

Full functionality (KATA and KEDR)

When using KATA and KEDR functionality, you can scan network traffic, mail traffic, and data on corporate LAN computers.

If more than 5,000 Endpoint Sensors components are installed within the organization, it is not recommended to use the Central Node component to process traffic.

You can use the Sensor component as a proxy server for connecting Endpoint Sensors and Central Node components. One Sensor component supports the connection of up to 1,000 Endpoint Sensors components.

The criteria for selecting a deployment scenario when using KATA and KEDR functionality are presented in the table below. The selection algorithm is as follows:

1. In each row of the table, select the cell containing the value of the criterion corresponding to your IT infrastructure.
If a row contains two cells with identical values, you must select the cell on the left.
2. Select the right-most column in which there are marked cells.

Table 3. Selecting a deployment scenario when using KATA and KEDR functionality

Criterion	Two-server scenario (see page 33)	Three-server scenario (see page 34)	Four- or more server scenario (see page 35)	Distributed solution (see page 43)
Network traffic and mail traffic cannot be received on the same device.	None	Yes	Yes	Yes
Number of Endpoint Sensors components	None	From 5000 to 10000	From 5000 to 10000	Over 10000
Communication channel bandwidth	1 Gbps	From 1 to 2 Gbps	Over 2 Gbps	Over 2 Gbps
The number of remote infrastructures in which traffic needs to be analyzed.	None	One	Two or more	Two or more
The capacities of one Sandbox component are insufficient to analyze all objects within acceptable time frames.	None	None	Yes	Yes

In distributed solution mode each program component must meet the hardware requirements specified in the sizing calculator.

Processing of network traffic, mail traffic, and web traffic (KATA)

It is recommended to use KATA functionality if the organization does not need to process data on corporate LAN computers. If this is the case, only network traffic and mail traffic are processed.

The criteria for selecting a deployment scenario when using KATA functionality are presented in the table below. The selection algorithm is as follows:

1. In each row of the table, select the cell containing the value of the criterion corresponding to your IT infrastructure.
If a row contains two cells with identical values, you must select the cell on the left.
2. Select the right-most column in which there are marked cells.

Table 4. Selecting a deployment scenario when using KATA functionality

Criterion	Two-server scenario (see page 33)	Three-server scenario (see page 34)	Four- or more server scenario (see page 35)
Network traffic and mail traffic cannot be received on the same device.	None	Yes	Yes
Communication channel bandwidth	1 Gbps	From 1 to 2 Gbps	Over 2 Gbps
The number of remote infrastructures in which traffic needs to be analyzed.	None	One	Two or more
The capacities of one Sandbox component are insufficient to analyze all objects within acceptable time frames.	None	None	Yes

Processing of data from corporate LAN computers (KEDR)

It is recommended to use KEDR functionality if the organization does not need to process traffic. If this is the case, only data on corporate LAN computers is processed.

Depending on the presence of a third-party Sandbox solution within the organization, you can use one of the following deployment scenarios:

- Without a Sandbox component (see page [35](#))
- With a Sandbox component (see page [36](#))

Two-server deployment scenario

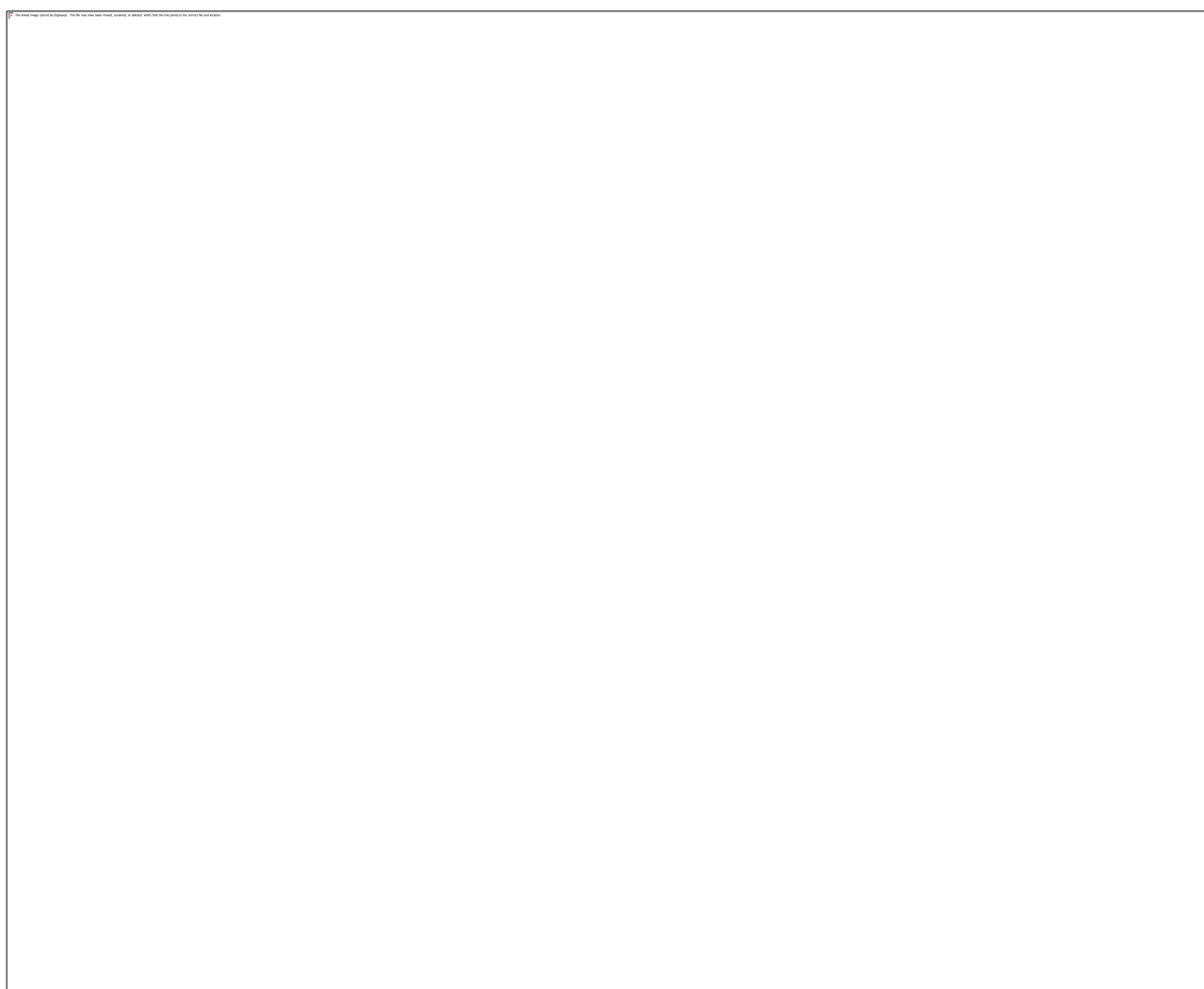
When using KATA and KEDR functionality, you can install Endpoint Sensors components to corporate LAN computers. When using KATA functionality, Endpoint Sensors components are not installed.

When this deployment scenario is used, the components required for use of KATA functionality are installed on two servers.

Sensor and Central Node components are installed on one same server. This server receives traffic, performs an initial analysis of traffic and a deeper analysis of extracted files. Based on the scan results, components detect signs of targeted attacks on the organization's IT infrastructure.

The Sandbox component is installed on the other server.

The scenario for program operation when deployed on two servers is presented in the figure below.



Scenario 1: Program operating scenario when deployed on two servers

Three-server deployment scenario.

When using KATA and KEDR functionality, you can install Endpoint Sensors components to corporate LAN computers. When using KATA functionality, Endpoint Sensors components are not installed.

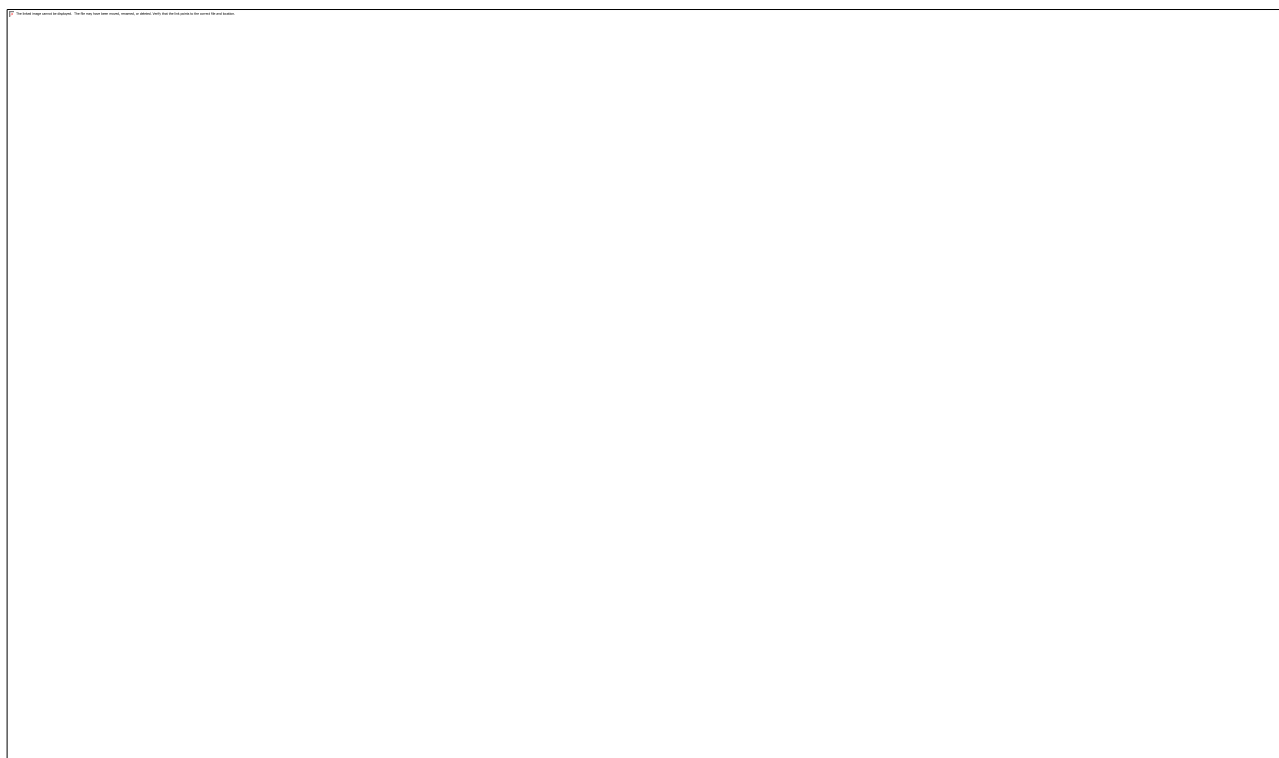
The Central Node component is always installed together with the Sensor component. If you need to use the Central Node component separately, do not configure the Sensor component.

When using this deployment scenario, the Sensor, Central Node and Sandbox components are installed on separate servers. The server with the Sensor component receives traffic, performs an initial analysis, extracts files and forwards them to the server with the Central Node component for a deeper analysis.

Using this deployment scenario, the Central Node component can receive traffic and perform an initial analysis of data in the main infrastructure. In this case, you can install the Sensor component on a server of a remote infrastructure whose traffic needs to be analyzed. If the channel bandwidth in the main infrastructure is more than 2 Gbps, you are advised to install the server with the Sensor component in the main infrastructure.

The traffic between the Central Node and Sensor components comprises up to 20% of traffic received by the Sensor component.

The program operating scenario when deployed on three servers is presented in the figure below.



Scenario 2: Program operating scenario when deployed on three servers

Scenario of deployment on four or more servers.

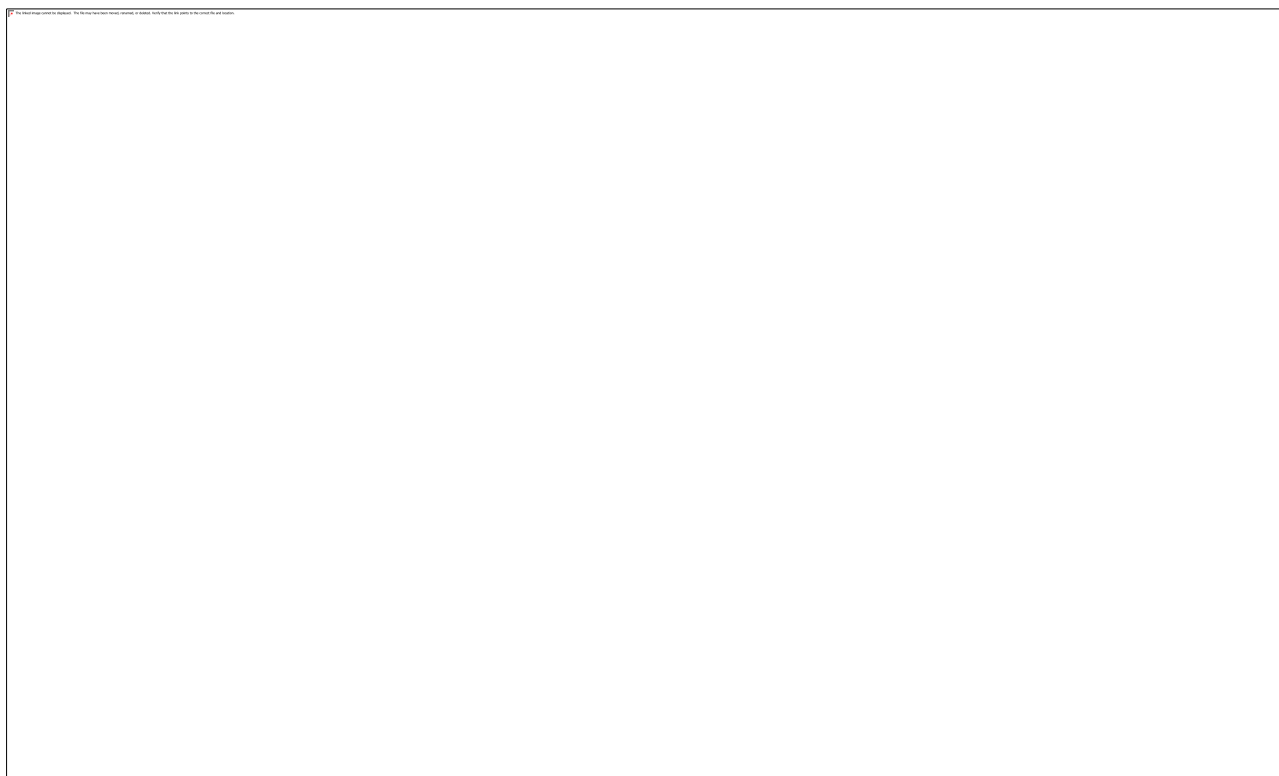
When using KATA and KEDR functionality, you can install Endpoint Sensors components to corporate LAN computers. When using KATA functionality, Endpoint Sensors components are not installed.

The Central Node component is always installed together with the Sensor component. If you need to use the Central Node component separately, do not configure the Sensor component.

If there is a large volume of traffic, you can install multiple Sensor components or multiple Sandbox components on different servers. This scenario is recommended for deployment in large organizations.

You can also use one Sandbox component to connect to multiple Central Node components.

The program operating scenarios when deployed on four or more servers are presented in the figure below.



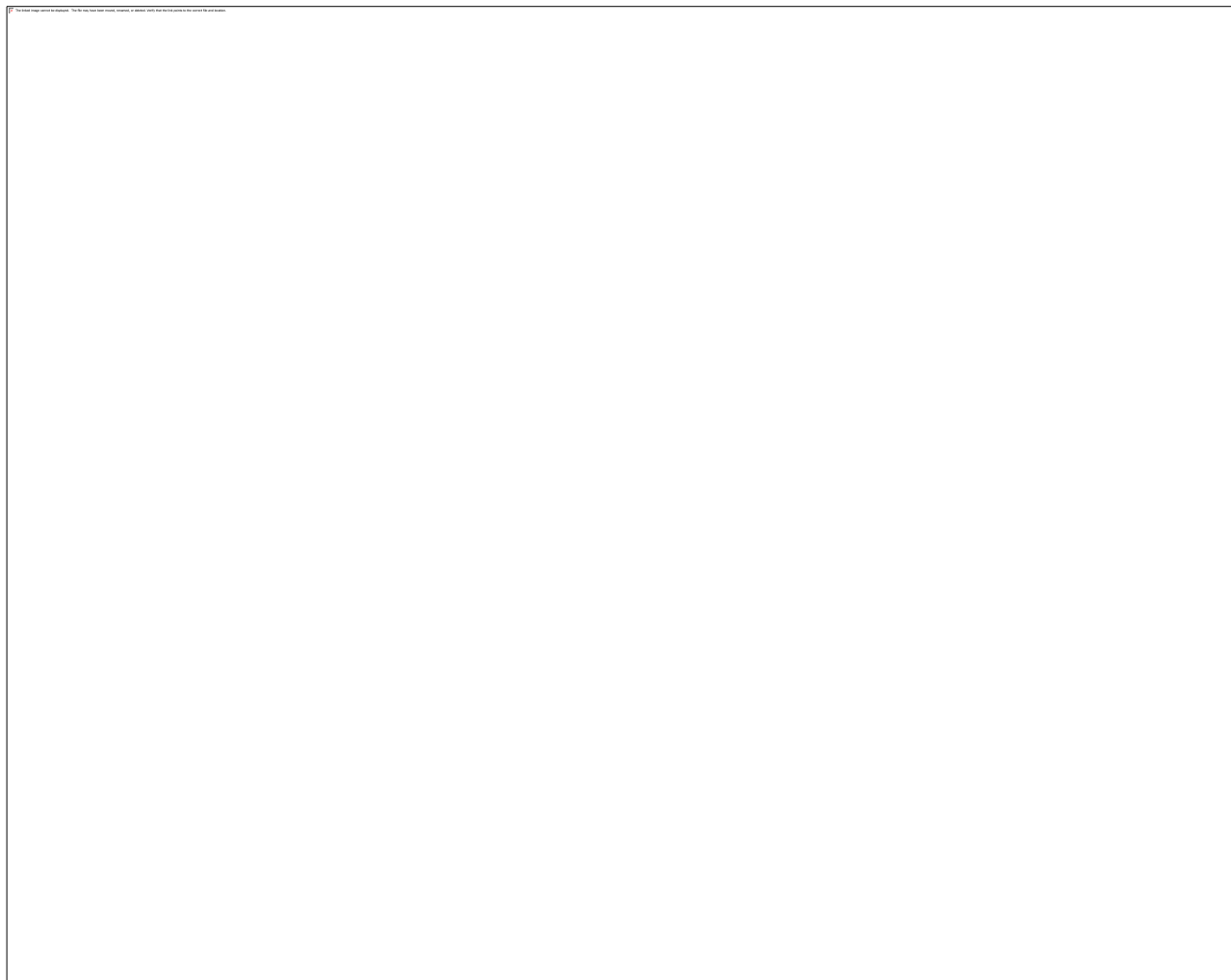
Scenario3: Program operating scenario when deployed on four or more servers

Scenario for deploying KEDR functionality without a Sandbox component

The Central Node component is always installed together with the Sensor component. If you need to use the Central Node component separately, do not configure the Sensor component.

Under this scenario, the Central Node component is required for managing Endpoint Sensors components and data analysis.

The program operating scenario when deploying KEDR functionality without the Sandbox component is presented in the figure below.



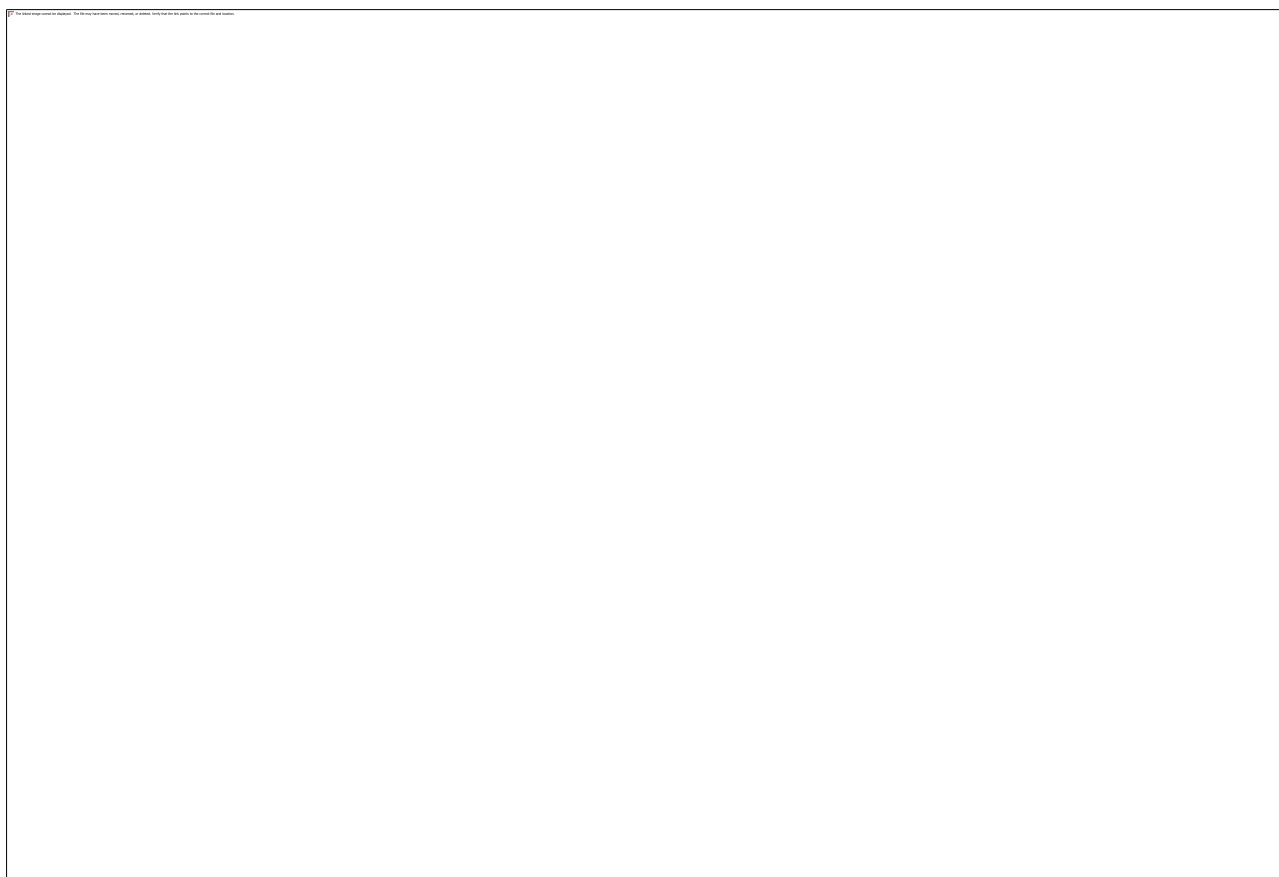
Scenario 4: Program operating scenario when deploying KEDR functionality without the Sandbox component

Scenario for deploying KEDR functionality with a Sandbox component

The Central Node component is always installed together with the Sensor component. If you need to use the Central Node component separately, do not configure the Sensor component.

Under this scenario, the Central Node component is required for managing Endpoint Sensors components and data analysis.

The program operating scenario when deploying KEDR functionality with the Sandbox component is presented in the figure below.



Scenario 5: Program operating scenario when deploying KEDR functionality with the Sandbox component

Program architecture

The program includes the following main components:

- *Sensor*. Receives data.
- *Central Node*. Scans data, analyzes the behavior of objects, and publishes analysis results in the web interface of the program.
- *Sandbox*. Starts virtual images of operating systems. Starts files in these operating systems and tracks the behavior of files in each operating system to detect malicious activity and signs of targeted attacks to the corporate IT infrastructure.
- *Endpoint Sensors*. Installed on separate computers that belong to the corporate IT infrastructure and run the Microsoft Windows operating system. Continuously monitors processes running on those computers, active network connections, and files that are modified.

Sensor component

The following modules of Kaspersky Anti Targeted Attack Platform run on each server hosting the Sensor component:

- *Sensor*. Receives data from network and mail traffic and sends the data for processing to the server with the Central Node component.
- *Intrusion Detection System* (hereinafter also referred to as *IDS*). Scans the Internet traffic for signs of intrusions into the corporate IT infrastructure.
- *KSN*. Checks the reputation of files and URL addresses in the Knowledge Base of Kaspersky Security Network on behalf of Kaspersky Anti Targeted Attack Platform and provides information about categories of websites (for example, malicious website, phishing website).

Kaspersky Security Network (hereinafter also "*KSN*") is an infrastructure of online services that provides access to Kaspersky Lab's online Knowledge Base with information on the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

If you do not want to participate in KSN, you can use *Kaspersky Private Security Network* (hereinafter also referred to as *KPSN*). KPSN is a solution that allows users to access the reputation databases of Kaspersky Security Network and other statistical data without actually sending data from their own computers to Kaspersky Security Network.

- *URL Reputation*. Detects malicious and phishing URL addresses, and URL addresses that were previously used by hackers in targeted attacks against and intrusions into the corporate IT infrastructure.

A Sensor component can also be a mail sensor (see page [213](#)), which is a server or virtual machine on which the Kaspersky Lab application Kaspersky Secure Mail Gateway (KSMG) or Kaspersky Security for Linux Mail Server (KLMS) is installed. These applications send email messages to Kaspersky Anti Targeted Attack Platform for processing. Based on the results of processing of email messages in Kaspersky Anti Targeted Attack Platform, KSMG and KLMS may block the transfer of messages.

If KSMG or KLMS is being used as a Sensor component, white lists configured for message recipients and MD5 checksums of files are not transmitted to KSMG and KLMS and are not applied when messages are processed by KSMG and KLMS.

Central Node component

The following modules, engines, and technologies of Kaspersky Anti Targeted Attack Platform run on each server hosting the Central Node component:

- *Anti-Malware Engine* (hereinafter also referred to as *AM* or *AM Engine*). Scans files and objects for viruses and other threats to the corporate IT infrastructure using anti-virus databases.
- *Mobile Attack Analyzer* (also referred to as *MAA*). Scans executable files in the APK format in the cloud infrastructure using a machine learning technology. As a result of the scan, Kaspersky Anti Targeted Attack Platform receives information about detected threats or absence of threats.
- *YARA*. Scans files and objects for signs of targeted attacks on the corporate IT infrastructure using YARA Rules databases created by users of Kaspersky Anti Targeted Attack Platform.
- *Targeted Attack Analyzer* (hereinafter also referred to as *TAA* or *TA Analyzer*). Performs statistical analysis and monitors network activity of software installed on computers of the corporate LAN. Searches for signs of network activity that the user of Kaspersky Anti Targeted Attack Platform is advised to direct his/her attention, as well as signs of targeted attacks to the corporate IT infrastructure.
- *KSN*. Checks the reputation of files and URL addresses in the Knowledge Base of Kaspersky Security Network on behalf of Kaspersky Anti Targeted Attack Platform and provides information about categories of websites (for example, malicious website, phishing website).

Sandbox component

Virtual images of the following operating systems are started on servers hosting the Sandbox component:

- Windows XP SP3, 32-bit.
- Windows 7, 64-bit.
- Windows 10, 64-bit.

The Sandbox component starts objects in these operating systems and analyzes the behavior of the objects to detect malicious activity and signs of targeted attacks to the corporate IT infrastructure.

By default, the maximum file size scanned by the Sandbox module is 100 MB. You can configure scan settings in the administrator menu of the program management console.
The maximum level of nesting for scanned archives is 32.

The maximum number of objects that can be in queue to be scanned by the Sandbox component per day is 10,000 objects. When this limit is reached, the program deletes 10% of the objects that have been queued for scanning the longest and replaces them with new objects queued for scanning. The deleted objects are saved in the program with the status NOT_SCANNED.

Endpoint Sensors component

The Endpoint Sensors component is installed on separate computers that belong to the corporate IT infrastructure and run the Microsoft Windows operating system (hereinafter also referred to as "corporate LAN computers" or simply "computers"). On these computers, the component continually monitors processes, active network connections, and files that are modified, and sends this monitoring data to the server with the Central Node component. Based on the results from this data being scanned by the Central Node component, the Endpoint Sensors component can also send files associated with detected events to the server with the Central Node component.

Computers intended for installation of the Endpoint Sensors component must meet the hardware and software requirements.

The Kaspersky Endpoint Security program component by Kaspersky Lab can also be used as an Endpoint Sensors component. Endpoint Sensors that are part of Kaspersky Endpoint Security can monitor processes, active network connections, and files that are modified, and send monitoring data to the server with the Central Node component.

If you install Kaspersky Endpoint Security on a computer that has the Endpoint Sensor component, the Endpoint Sensor component will be removed regardless of whether or not the Endpoint Sensor component is included in Kaspersky Endpoint Security.

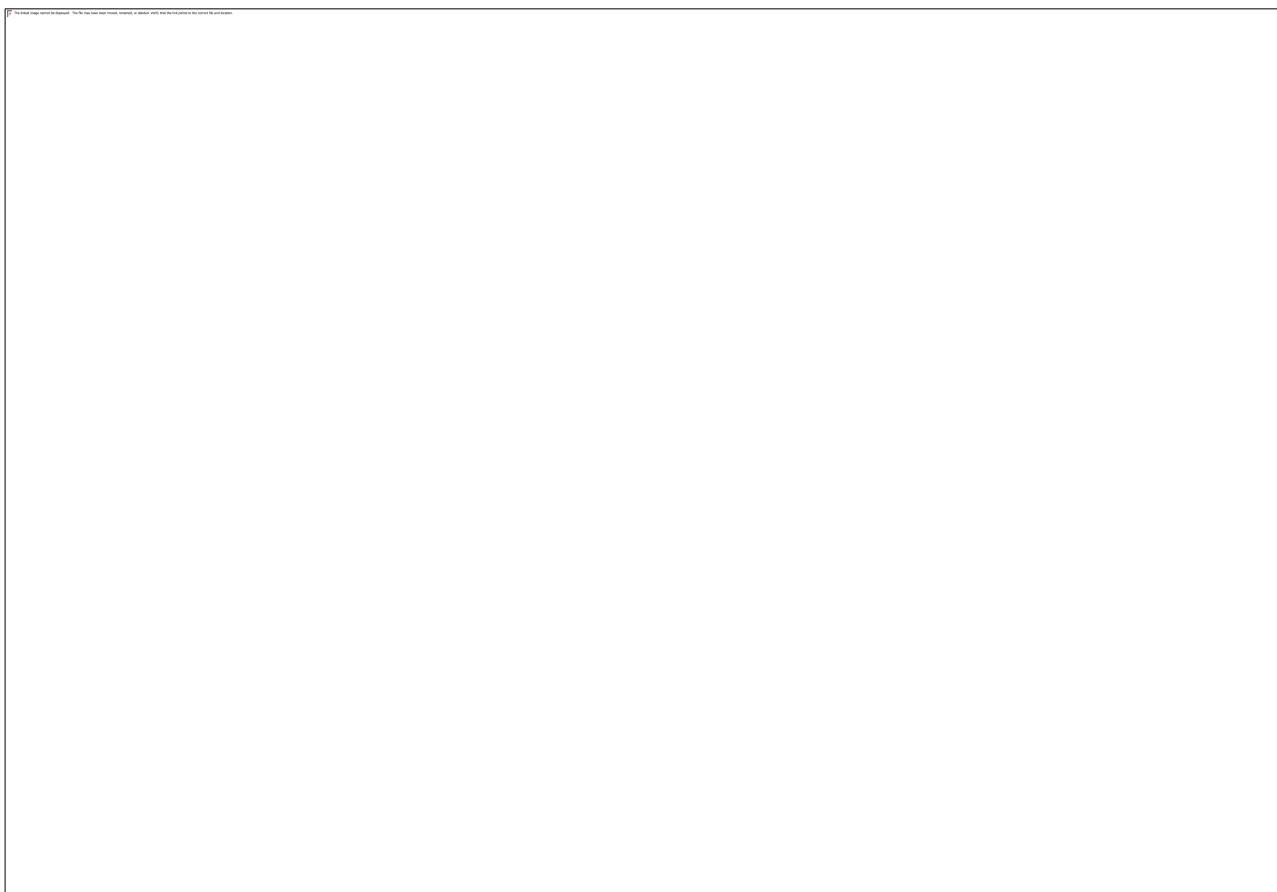
In addition, Kaspersky Anti Targeted Attack Platform can be integrated with Kaspersky Security Center and receive statistics on the operation of the Endpoint Sensors component.

Operation of the program

After its integration into the corporate IT infrastructure, the program publishes information about detected signs of targeted attacks and intrusions into the corporate IT infrastructure in the web interface.

You can configure settings of each Central Node component individually or manage several components in a centralized way in distributed solution mode.

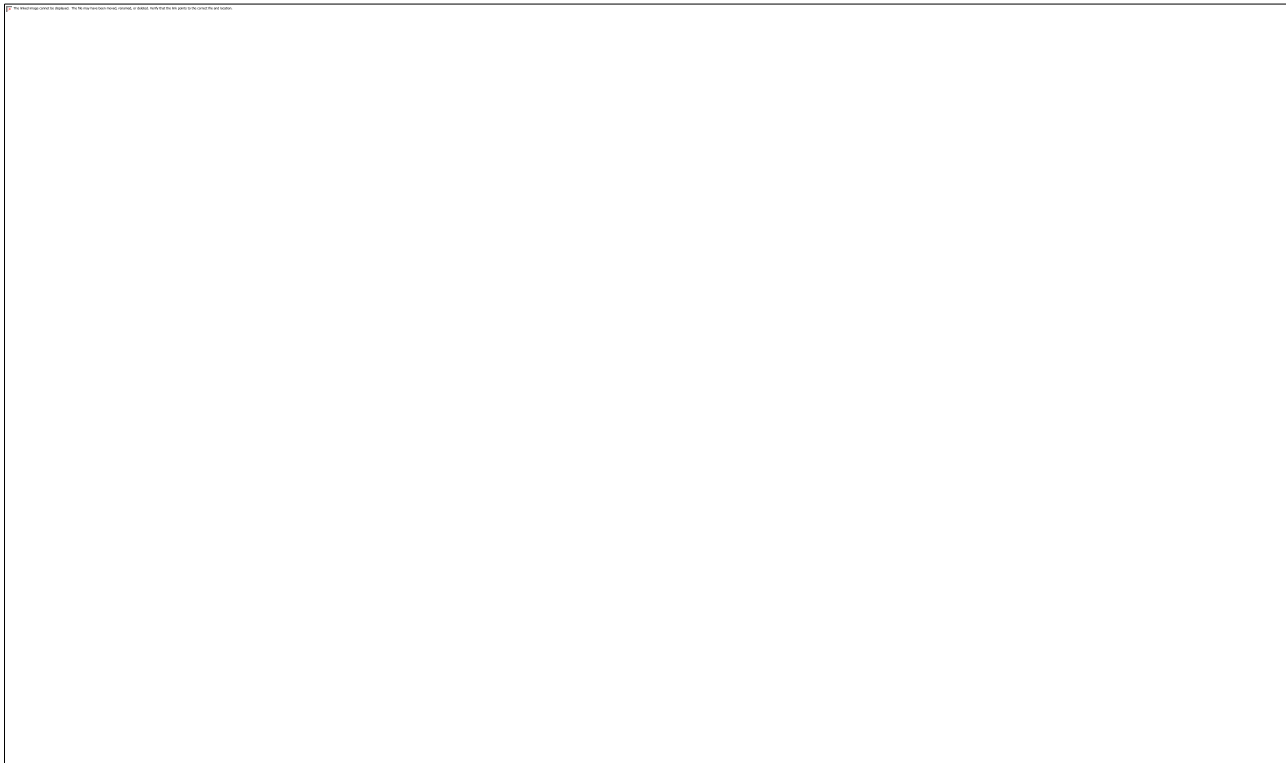
The program's operating scheme is shown in the figure below.



Scenario 6: Operation of the program in standalone solution mode

A distributed solution (see page [43](#)) is a two-tier hierarchy of Central Node servers. This structure sets apart a master control server known as the *Primary Central Node (PCN)* and slave servers known as *Secondary Central Nodes (SCN)*.

The principle of operation of the program in distributed solution mode is shown in the figure below.



Scenario 7: Operating scheme of the program in distributed solution mode

Distributed solution and multitenancy mode

You can configure settings of each Central Node component individually or manage several components in a centralized way in distributed solution mode.

The distributed solution is a two-tier hierarchy of servers with Central Node components installed. This structure sets apart a master control server known as the *Primary Central Node (PCN)* and slave servers known as *Secondary Central Nodes (SCN)*. Interaction of servers requires connecting SCN to PCN.

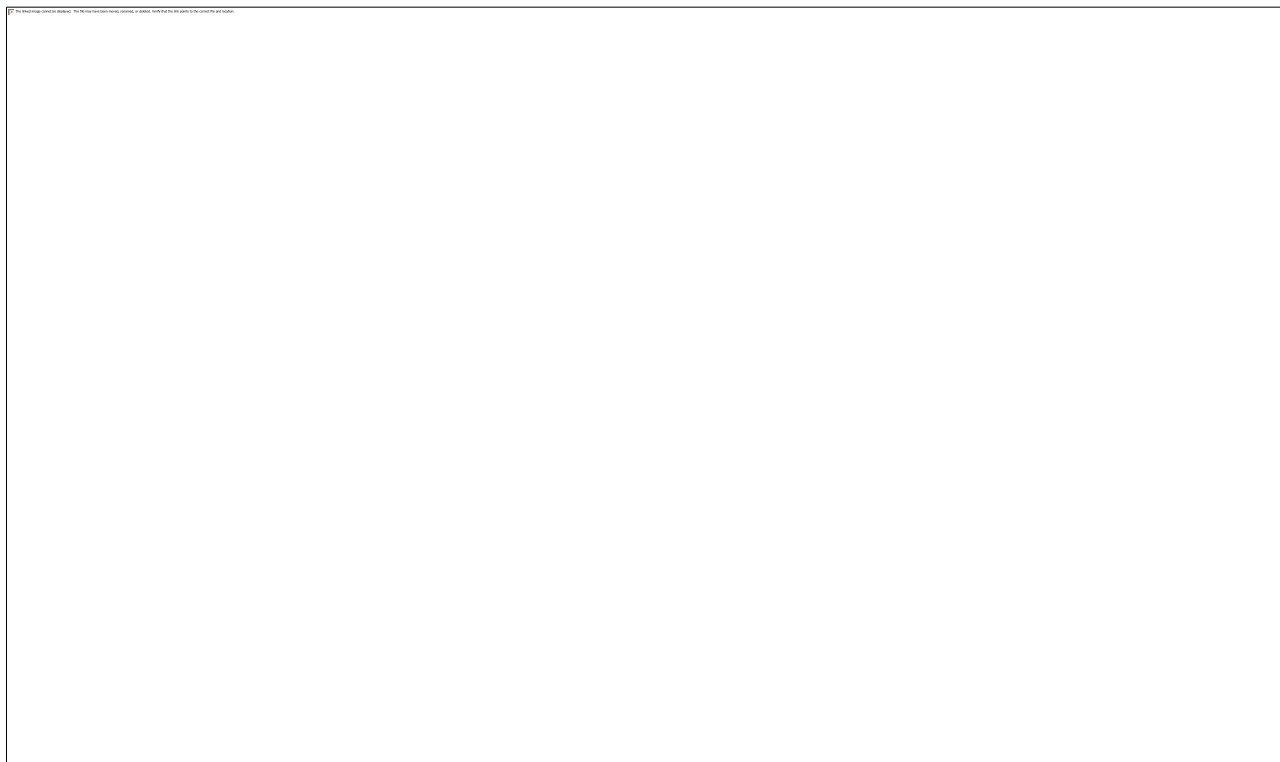
PCN and SCN scan files and objects using the same technology as the individually managed Central Node component.

The distributed solution allows centralized management of the following functional areas of the program:

- Users.
- Alerts.
- Threat Hunting.
- Tasks.
- Prevention.
- IOC/IOA Analysis.
- Storage.
- Endpoint Sensors, including network isolation of hosts.
- Reports.

If you support multiple organization, you can use the program in the multitenancy mode. You can install Kaspersky Anti Targeted Attack Platform on one or more Central Node for each organization. Each organization has its own

PCN server and SCN servers connected to it. Each organization can manage the program independently from other organizations. The provider can manage data of several organizations.



You can use distributed solution and multitenancy mode in the following cases:

- To protect more than 10,000 hosts in an organization.
- For centralized management of the program in different departments of the organization;
- For centralized management of the program on servers of multiple organizations.

After you switch the program to distributed solution and multitenancy mode, license key management is only available on the PCN. All keys added to the SCN before are deleted. Each connected SCN receives a key from the PCN.

You can deploy the program in distributed solution and multitenancy mode in the following scenarios:

- Install the Central Node component on new servers and assign PCN and SCN roles to those servers.
- Assign PCN and SCN roles to servers that already have the Central Node component installed.

In this case you must update the Central Node component to version 3.6.

Before you switch servers with Central Node components installed to distributed solution mode, review the changes that will be applied to the system after the operating mode is changed. Assigning the PCN role to a server is irreversible.

Distributed mode and multitenancy transition scenario

Switching the program to distributed solution mode and multitenancy mode involves the following steps:

- a. Installing the Central Node components (see page [105](#))
- b. Assigning the PCN role to one of the servers (see page [49](#))
- c. Assigning the SCN role to the rest of the servers and sending requests to connect to the PCN (see page [50](#))
- d. Processing a SCN to PCN connection request (see page [50](#))

Modifications of program settings for distributed solution mode and multitenancy

Modifications of program settings for the distributed solution mode and multitenancy mode are shown in the following table.

Table 5. Modifications of program settings for the distributed solution mode and multitenancy

mode

Functional area	PCN	SCN
Users	Users and roles assigned to them are preserved. Additionally, PCN users are granted access rights to work with PCN and all connected SCNs.	<p>All users are deleted except the user that was created while Central Node was deployed.</p> <p>After that, the SCN requests a list of users from the PCN and uses that list to create local users with the same parameters:</p> <ul style="list-style-type: none"> • Name • Password • Role • Status <p>Users that do not have rights to access the SCN, are not displayed in the list of users.</p>
Alerts	Information about all alerts from all connected SCNs is added to the PCN database.	The user name is no longer displayed in existing alert information. User data are deleted from alert operation history.
Dashboard	<p>On the Alerts tab, you can now select the SCNs whose information should be displayed in the widget.</p> <p>On the System health tab, the status of connection of the PCN with connected SCNs is now displayed.</p>	On the System health tab, the status of connection with the PCN is now displayed.
Tasks	<p>Tasks created on the Central Node server before it was assigned the PCN role, as well as tasks created on the PCN after switching to distributed solution mode, apply to all connected SCNs.</p> <p>Tasks created on SCNs are also displayed in the task list. Settings of these tasks cannot be changed on the PCN.</p>	<p>Tasks created on the PCN are displayed, as well as tasks created on this SCN.</p> <p>Settings of tasks created on the PCN cannot be changed.</p>

Functional area	PCN	SCN
Reports	<p>Templates and reports created before the switch to distributed solution mode are preserved.</p> <p>A Servers column is added to the report table, containing information about the relevant SCN for the alert.</p> <p>After switching to distributed solution mode, only reports created on the PCN are displayed.</p>	<p>Templates and reports created before the switch to distributed solution mode are preserved.</p> <p>Information about the user who created the report is preserved if the PCN has a user with the same ID (guid). In other cases user information is deleted.</p> <p>After switching to distributed solution mode, only reports created on an SCN are displayed.</p>
Prevention	<p>Policies created on the Central Node server before it was assigned the PCN role, as well as policies created on the PCN after switching to distributed solution mode, apply to all connected SCNs.</p> <p>Policies created on SCNs are also displayed in the policy list.</p> <p>Settings of these policies cannot be changed on the PCN.</p>	<p>Policies created on the PCN are displayed, as well as policies created on this SCN.</p> <p>Settings of policies created on the PCN cannot be changed.</p>
Storage	<p>All files and metadata that were stored on the PCN before the switch to distributed solution mode are preserved. The name of the PCN is displayed for them in the Central Node column.</p> <p>The PCN also keeps the contents of the Backup of all connected SCNs.</p>	<p>All files and metadata that were stored on SCNs before the switch to distributed solution mode are preserved.</p>
White List	No changes.	No changes.
VIP Status	No changes.	No changes.
Notifications	No changes.	No changes.
Integration with mail sensors	No changes.	No changes.
Integration with Kaspersky Security Center	Integration with Kaspersky Security Center becomes unavailable.	Integration with Kaspersky Security Center becomes unavailable.
Threat Hunting	<p>During threat hunting in the database, the PCN sends a request to all connected SCNs.</p> <p>After the search query is processed, a list of PCN and SCN events of the selected organization is displayed.</p>	No changes.

Functional area	PCN	SCN
IOC/IOA Analysis	IOC files added on the Central Node server before it was assigned the PCN role are applied to the PCN. IOA rules added on the Central Node server before it was assigned the PCN role are applied to the PCN.	IOC files and IOA rules added on the PCN, as well as IOC files and IOA rules added on this SCN before and after switching to distributed solution mode are displayed.
Backup of the program	If any SCNs are connected, backup on the PCN becomes unavailable.	Backup of the program becomes unavailable.

Assigning the PCN role to a server

Assigning the PCN role to a server is irreversible. After changing the server role to PCN, you will not be able to change the role of that server to SCN or standalone server. To change the role of that server you will have to reinstall the program.

► To assign the PCN role to a server:

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the server to which you want to assign the PCN role.
2. Select the **Operation mode** section.
3. Click the **Distributed solution** button.
4. In the **Server role** drop-down list, select **Primary Central Node**.
5. In the **Company name** field, enter the name of the organization to which this Central Node server belongs.
6. Click the **Assign the PCN role** button.

The action confirmation window opens.

After confirming the action, log in to the program web interface again.

7. Click **Yes**.

The server is assigned the PCN role and the name of the organization.

After logging in to the program web interface with administrator credentials, the **Operation mode** section of the program web interface displays the following information:

- **Current mode** – Distributed solution.
- **Server role** – Primary Central Node.
- **Certificate fingerprint** – the fingerprint of the server's certificate required for authentication when establishing connection with an SCN.

- **Companies** – information about organizations to which this server belongs, and about connected SCN servers:
 - **IP** – Primary Central Node for this server and IP addresses of SCN servers (after they connect).
 - **Server** – name of this server and names of SCN servers (after they connect).
This name is not related to name of the host where the program is installed. You can change it.
 - **Certificate fingerprint** – blank value for this server and certificate fingerprints of SCN servers (after they connect).
 - **Status** – connection state of SCN servers (after they connect) and the number of servers in the organization.
- The **Servers pending authorization** table contains information about connected SCN (see page [51](#)).

Assigning the SCN role to a server

► *To assign the SCN role to a server:*

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the server to which you want to assign the SCN role.
2. Select the **Operation mode** section in the window of the program web interface.
3. Click the **Distributed solution** button.
4. In the **Server role** drop-down list, select **Secondary Central Node**.
5. In the **PCN IP** field, enter the IP address of the server that has the PCN role, to which you want to connect the SCN.
6. Click **Get certificate fingerprint**.
A fingerprint of the certificate of the server that has the PCN role is displayed in the workspace.
7. Contact the administrator of the PCN and compare the certificate fingerprint you received with the fingerprint displayed on the PCN in the **Certificate fingerprint** field of the **Operation mode** section.
8. If certificate fingerprints on the SCN and the PCN match, click **Send connection request**.
The action confirmation window opens.
9. Click **Yes**.

The server is assigned the SCN role after the PCN administrator accepts the connection request. The SCN server will be assigned to the organization specified by the PCN administrator.

Processing SCN to PCN connection requests

► *To create a request for connection of the SCN to the PCN:*

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the PCN server that you want to use to process connection requests from other servers.
2. Select the **Operation mode** section in the window of the program web interface.

The workspace displays the **Servers pending authorization** table.

3. Contact the SCN administrator who sent the connection request and verify the certificate fingerprint in the **Servers pending authorization** table. It must match the fingerprint displayed on the SCN in the **Request certificate fingerprint** field of the **Operation mode** section.
4. If certificate fingerprints on the PCN and the SCN match, do one of the following:
 - If you want to reject the connection request from the SCN, click **Reject**.
 - If you want to accept the connection request from the SCN:
 1. Click **Accept**.
The **Accept connection request** window opens.
 2. In the **Company** list, select the organization to which you want to assign this SCN server. The list includes organization that have been added before (see page [52](#)).
 3. Click **Accept**.

Accepting connection requests is not recommended if certificate fingerprints do not match. Make sure the data you entered is correct.

If you reject the connection request, the SCN will continue to operate as a standalone Central Node server.

Viewing information about organizations, PCN and SCN servers

In the web interface of the PCN server, you can view information about this server and about all SCN servers that are connected to it.

► *To view information about organizations, PCN and SCN servers in multitenancy mode:*

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the PCN server.
2. Select the **Operation mode** section in the window of the program web interface.

The workspace displays the following information about organizations and servers:

- **Current mode** – Distributed solution.
- **Server role** – Primary Central Node.
- **Certificate fingerprint** – certificate fingerprint of the PCN server.
- **Companies** – information about organizations to which the server belongs, as well as all SCN servers that connect to the PCN.
 - **IP** – Primary Central Node for the PCN server and IP addresses of SCN servers connected to the PCN.
 - **Server** – name of the server and names of SCN servers that connect to the PCN.
This name is not related to name of the host where the program is installed. You can change it.
 - **Certificate fingerprint** – blank value for the PCN server and certificate fingerprints of SCN servers waiting to connect to the PCN.

- **Status** – connection state and the number of servers in the organization.
- The **Servers pending authorization** table contains the following information:
 - **IP** – IP address or domain name of the SCN server.
 - **Server** – name of the SCN server that is displayed in the program web interface.
This name is not related to name of the host where the program is installed. You can change it.
 - **Certificate fingerprint** – certificate fingerprint of the SCN server that is sent to the PCN with the connection request.
 - **Status** – status of the SCN to PCN connection.

Adding an organization to the PCN server

► *To add an organization in the PCN server web interface:*

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the PCN server for which you want to add an organization.
2. Select the **Operation mode** section in the window of the program web interface.
3. In the right part of the **Companies** workspace, click **Add**.
4. In the **Name** field, enter the name of the organization that you want to add.
5. Click the **Add** button.

The organization is added and shown in the list.

Removing an organization from the PCN server

► *To delete an organization in the PCN server web interface:*

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the PCN server for which you want to delete an organization.
2. Select the **Operation mode** section in the window of the program web interface.
3. In the **Companies** workspace, select the organization that you want to delete.
4. Click the **Delete** button.

The action confirmation window opens.


The action is irreversible. All global objects as well as reports and report templates of this organization are lost.

5. Click **Yes**.

The organization is deleted.

Renaming an organization on the PCN server

► *To change the name of an organization in the web interface of the PCN server:*

1. Log in to the program web interface with the administrator account.
You need to log in to the web interface of the PCN server for which you want to change the name of an organization.
2. Select the **Operation mode** section in the window of the program web interface.
3. In the **Companies** list, click  next to the organization that you want to rename.
This opens a window in which you can change the name of the organization.
4. In the **Name** field, change the name of the organization.
5. Click the **Save** button.

The name of the organization is changed.

Disconnecting an SCN from PCN

The SCN can be disconnected from the PCN unilaterally.

If you disconnect an SCN using the SCN web interface, changed settings are only applied to the SCN. The PCN continues to display information about that server.

If you disconnect the SCN using the PCN web interface, information about that server is deleted at the PCN. However, the server with the SCN role will keep trying to connect to the PCN to synchronize settings.

To complete a bilateral disconnect, you must follow both instructions presented below. In this case, the SCN keeps working as a standalone Central Node server, and information about the disconnected SCN is displayed on the PCN.

The administrator of Kaspersky Anti Targeted Attack Platform is responsible for the confidentiality of data on PCN, SCN, and Central Node servers. If you plan to move an SCN server from one organization to another, delete all data remaining on the server after using Kaspersky Anti Targeted Attack Platform and reinstall Kaspersky Anti Targeted Attack Platform before handing over the server to the different organization.

► *To disconnect the SCN from the PCN using the PCN web interface:*

1. Log in to the program web interface with the administrator account.
Log in to the web interface of the PCN server that you want to disconnect the SCN from.
2. Select the **Operation mode** section in the window of the program web interface.
3. In the server list, select the SCN that you want to disconnect.
4. Click **Disconnect**.
The action confirmation window opens.
5. Click **Yes**.

The SCN will attempt to connect to the PCN to synchronize settings.

► *To disconnect the SCN from the PCN using the SCN web interface:*

1. Log in to the program web interface with the administrator account.
Log in to the web interface of the SCN server that you want to disconnect from the PCN.
2. Select the **Operation mode** section in the window of the program web interface.
3. Click **Disconnect**.
The action confirmation window opens.
4. Click **Yes**.

The SCN is disconnected from the PCN and continues working as a standalone Central Node server.

Modifications of program settings for disconnecting an SCN from PCN

Modifications of program settings after an SCN is disconnected from the PCN are listed in the following table.

Table 6. *Modifications of program settings after disconnecting an SCN from PCN*

Functional area	PCN	SCN
Users	The disconnected SCN is not removed from the list of servers to which user rights apply. Information about changes of the user account that has rights on the disconnected SCN is not sent to the SCN.	User accounts received from the PCN are not deleted. You can create new user accounts again, as well as disable and change passwords for existing user accounts.
Alerts	Alert information on the disconnected SCN is deleted.	Operation history and all alert information is preserved.
Tasks	Tasks created on the disconnected SCN are deleted.	Tasks created on the PCN are deleted. Information about users who created tasks on the SCN is preserved.
Reports	All reports created earlier concerning the disconnected SCN are preserved, as well as the ability to filter the report list by this server.	Templates and reports are not modified.
Prevention	Policies created on the disconnected SCN are deleted.	Policies created on the PCN are deleted. Information about users who created policies on the SCN is preserved.
Storage	All objects related to the disconnected SCN are deleted from Backup.	All objects in the Backup are preserved. The link to the task stops working in information about objects received as part of tasks created on the PCN.
White List	No changes.	No changes.
VIP Status	No changes.	No changes.
Notifications	No changes.	No changes.
Integration with mail sensors	No changes.	No changes.
Integration with Kaspersky Security Center	Configuring integration with Kaspersky Security Center stays unavailable.	Configuring integration with Kaspersky Security Center becomes available.
Threat Hunting	After the search query is processed, events related to the disconnected SCN are not displayed.	No changes.
IOC/IOA Analysis	IOC and IOA indicators of the disconnected SCN are deleted.	IOC and IOA indicators created on the PCN are deleted.

Functional area	PCN	SCN
Backup of the program	Backup of the program remains unavailable.	Backup of the program becomes available.

Decommissioning an SCN server

If you are not planning to subsequently use an SCN server, you can decommission the SCN server by deleting it from the PCN.

The administrator of Kaspersky Anti Targeted Attack Platform is responsible for the confidentiality of data on PCN, SCN, and Central Node servers. If you plan to move an SCN server from one organization to another, delete all data remaining on the server after using Kaspersky Anti Targeted Attack Platform and reinstall Kaspersky Anti Targeted Attack Platform before handing over the server to the different organization.

Decommissioning an SCN server consists of the following steps:

- a. **Deleting all data on the SCN**
- b. **Disconnecting the SCN from the PCN through the PCN web interface (see page [53](#))**
- c. **Disconnecting the SCN from the PCN through the SCN web interface (see page [53](#))**
- d. **Deleting the SCN through the PCN web interface**

► *To delete the SCN through the PCN web interface:*

1. Log in to the program web interface with the administrator account.
Log in to the web interface of the PCN server from which you want to delete the SCN.
2. Select the **Operation mode** section in the window of the program web interface.
3. In the server list, select the SCN that you want to delete.
4. Click the **Delete** button.
5. In the confirmation window, click **Yes**.

The SCN will be deleted. Information about the deleted SCN will no longer be displayed on the PCN.

About data provision

The operation of certain components of Kaspersky Anti Targeted Attack Platform requires data processing on the Kaspersky Lab side. Components do not send data without the consent of the administrator of Kaspersky Anti Targeted Attack Platform.

You can view the list of data and the terms on which it is used as well as give consent to data processing in the following agreements between your organization and Kaspersky Lab:

- In the End User License Agreement (for example, during installation of the program).
According to the terms of the End User License Agreement, you agree to automatically send Kaspersky Lab the information listed in the End User License Agreement under Data Provision. The End User License Agreement is included in the program distribution kit.
- In the KSN Statement (for example, during installation of the program or in the administrator menu after installation).

When you participate in Kaspersky Security Network, information obtained as a result of Kaspersky Anti Targeted Attack Platform operation is automatically sent to Kaspersky Lab. The list of transmitted data is specified in the KSN Statement. The Kaspersky Anti Targeted Attack Platform user independently decides on his/her participation in KSN. The KSN Statement is included in the program distribution kit.

Before KSN statistics are sent to Kaspersky Lab, they are accumulated in the cache on servers hosting Kaspersky Anti Targeted Attack Platform components.

Kaspersky Lab protects any information received in this way as prescribed by law and applicable rules of Kaspersky Lab.

Kaspersky Lab uses any received information in anonymized form and as general statistics only. General statistics are automatically generated using original collected information and do not contain any personal or other confidential data. The original information received is destroyed as new information is accumulated (once a year). General statistics are stored indefinitely.

When using Kaspersky Private Security Network, Kaspersky Lab is not sent information about the operation of Kaspersky Anti Targeted Attack Platform. However, KSN statistical data is accumulated in the cache on servers hosting Kaspersky Anti Targeted Attack Platform components to the same extent as when using Kaspersky Security Network. This accumulated KSN statistical data may be transmitted beyond the confines of your organization if a server with Kaspersky Private Security Network is located outside of your organization.

The Kaspersky Private Security Network administrator must personally ensure the security of such data.

Data of the Central Node and Sensor components

This section contains the following information about user data that is stored on the server with the Central Node component and on the server with the Sensor component:

- Contents of stored data
- Storage location
- Storage duration
- User access to data

Data in logs and trace files

Kaspersky Anti Targeted Attack Platform records user action logs and particular actions of the program components. Logs may contain all data displayed in the information about alerts, policies, events, tasks, and task results.

Data on the Central Node server is stored in open, non-encrypted form and is deleted on a rotational basis when the maximum allowed file size is reached. Logs store data for the last 7 days, and that data is permanently deleted when the program is uninstalled.

The Kaspersky Anti Targeted Attack Platform administrator must independently ensure the security of this data.

Kaspersky Anti Targeted Attack Platform writes data to the following logs:

1. Processing history log. This is stored in the file `/var/log/kaspersky/apt-history/apt-history.log` on the Central Node and Sensor servers. This log records the stages involved in processing objects, modifications made to settings, information about the completion of tasks and preventions, so that such information can be subsequently used for the purposes of troubleshooting and improving the quality of the program. The data that is written to the processing history log is listed below.
 - a. Information about a scanned file:
 - MD5 hash of the scanned file.
 - File processing date.
 - Scan result.
 - Version of the database used to scan the file.
 - Kernel that was involved in scanning the file.
 - b. Information about processing a file or URL based on a white list:
 - Name, type, size of the file, file path, MD5 hash and SHA256 hash of the file, and the URL from which the file was downloaded.
 - URL.
 - White list rule.
 - IP address and port of the computer that established the connection (client).
 - IP address and port of the computer from which the connection was established (server).

- Type of HTTP request (GET, POST).
 - Date and time of the request (with precision up to the second).
 - User Agent (browser data) of the client.
 - Referrer.
 - Type of DNS message (request, response).
 - Type of DNS request (A, MX).
 - Date and time of the DNS message (with precision up to the second).
 - List of all IP servers (for A-record DNS response).
 - List of all domain names of mail servers, and all IP addresses associated with the A-record (for MX-record DNS response).
 - Value of the triggered white list rule: email address, IP address, domain, type of file, and MD5 hash of the file.
- c. Information about processing an email according to the white list:
- Information about the message: email addresses of the sender and recipients.
 - Subject of the message.
- d. Instance of alert generation:
- Alert importance.
 - Date and time when the event is detected.
 - Modules and technologies employed to scan the file.
 - Results of the scan by modules and technologies.
 - MD5 hash of the scanned file.
 - Scanned URL.
- e. Creation of tasks for computers with the Endpoint Sensors component:
- Task ID, creation time, task execution timeout, and task type.
 - IP address, and name of the host to which the task is assigned.
 - Name, path to the requested file, and MD5 hash of the requested file.
 - Task priority.
- f. Processing of task execution results for computers with the Endpoint Sensors component:
- Path of the temporary file of the package from the computer with the Endpoint Sensors component, and package size.
 - Host name and IP address of the computer with the Endpoint Sensors component.
 - Version of the report from the computer with the Endpoint Sensors component.
 - Details of file scan results.
 - Process ID, and number of memory areas.
 - Indicator of successful task processing.

- Description of the error that occurred when processing tasks of the computer with the Endpoint Sensors component. In addition to technical information, the error description may contain the following user data:
 - Paths to files located on the computer with the Endpoint Sensors component.
 - Email messages: message body, attachments, email addresses of the sender and recipients of the message, IP address of the message sender, information contained in service headers of the message, and the email message ID.
 - Contents of files.
 - URLs extracted from the email message from which a file was downloaded or that the user clicked through.
 - User account name, IP address and name of the user's computer.
 - MachineID of the user's computer.
 - UID of the user's computer in KSC.
 - Unique ID of the computer from the Endpoint Sensors component.
 - MAC address of the user's computer.
- g. Policy management:
 - Prevention ID, data and time of modifications made to the prevention.
 - MD5- or SHA256 hash of the file.
 - Unique ID of the computer from the Endpoint Sensors component.
 - Prevention name.
 - MachineID of the host.
- 2. Audit log. This is stored in the file `/var/log/kaspersky/apt-audit.log` on the Central Node and Sensor servers. The log records actions taken on accounts, settings, and changes to the operating statuses of program components, so that such information can be subsequently used for troubleshooting purposes. The data that is written to the audit log is listed below.
 - a. Information about modifications to the white list:
 - User account name.
 - Value of the white list element: MD5 hash, format, URL mask, subnet, User Agent (browser data), and email address.
 - b. Statuses of program components:
 - Time, component name, IP address, status, and error description.
 - Database update status.
 - c. Actions on user accounts:
 - Event type (creation, modification, deletion).
 - Date and time.
 - User account name.
 - IP address of the user's computer.
 - User role.

- User status (active/user operations suspended).
- Name of the user account that made the modification.
- d. Modification to VIP group entries:
 - Event type.
 - Date and time.
 - Name of the user that created or modified the VIP group entry.
 - IP address, FQDN of the computer, and email address.
- e. Actions taken on alerts:
 - Alert ID.
 - Name of the user account that performed the action on the alert.
- 3. The system log and trace files are stored on the Central Node and Sensor servers. The system log is saved in the directory `/var/log`. Trace files are saved in the directory `/var/log/kaspersky`.

Trace files in open (non-encrypted) form may contain the same data that is included in the scope of data on alerts, policies, events, tasks, and task results. You can configure trace files to be written to syslog (in Technical Support Mode).

The system log records general information about the status of the program, as well as errors and exceptions in the operation of various components of the program (including from a third-party developer) and the operating system.

In addition to data on alerts, policies, events, tasks, and task results, trace files and system logs may also contain the following user data:

- a. Paths to files on the local computer.
- b. Email messages: message body, attachments, email addresses of the sender and recipients of the message, IP address of the message sender, information contained in service headers of the message, and the message ID.
- c. Contents of files.
- d. URL:
 - extracted from the email message
 - used to download a file
 - clicked through by the user
- e. User account name, IP address and name of the user's computer.
- f. MachineID of the user's computer.
- g. UID of the user's computer in KSC.
- h. Unique ID of the computer from the Endpoint Sensors component.
- i. MAC address of the user's computer.

Data in alerts

Alerts may contain user data. Information about alerts is stored on the server with the Central Node component in the directory `/data/var/lib/kaspersky/storage/pgsql/10/data/` and is rotated as disk space is filled. Files whose scan results generated an alert are accumulated on the server hosting the Central Node component and rotated as disk space is filled up.

Kaspersky Anti Targeted Attack Platform resources provide no capability to restrict the rights of the users of servers and operating systems to which the Central Node component is installed. The administrator is advised to use any system resources at their own discretion to control how the users of servers and operating systems with the program installed may be granted access to the personal data of other users.

The following information is stored in all alerts:

- Alert time.
- Date and time of alert modification.
- Category of the detected object.
- ID of the user to whom the alert is assigned.
- User comments added to the alert information.
- IP address and name of the computer on which the alert was generated.
- Unique ID of the computer on which the alert was generated.

If a file is detected in network traffic or mail traffic, the following information may be stored on the server:

- Name, size, and type of file.
- MD5- and SHA256 hash of the file.
- Category of the detected object (for example, name of the virus) and alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer security or corporate LAN security based on Kaspersky Lab experience.
- Versions of databases of Kaspersky Anti Targeted Attack Platform components that were used to generate the alert.
- For each virtual machine of the Sandbox component: virtual machine name, version of the Sandbox component database used to scan the file, and the file behavior analysis log.
- Names of YARA rules used to generate the alert.
- Object scan status by technology, and scan time for each technology.
- IP address and type of integration of the server on which the alert was generated.
- For IDS alerts: source address, destination address, URL, User Agent, and method.
- If the file was received from the Endpoint Sensors component: IP address, name, domain of the host (in FQDN format), full path to the file on the computer with the Endpoint Sensors component, and the file name.
- VIP group affiliation.
- DNS request, response to the request, and list of hosts from the request.
- URL of the FTP request.

If an email message was detected, the following information may be stored on the server:

- Email addresses of the sender and recipients of the message (including the recipients of copies and blind carbon copies of the message).
- Subject of the email message.

- Date and time when the message was received by Kaspersky Anti Targeted Attack Platform, with precision up to the second.
- Unique ID of the email message.
- All service headers of the message (as they appear in the message).
- IP address, name, and integration type of the server on which the email message was detected.
- URL extracted from the email message.

If the alert was generated by URL Reputation technology, the following information may be stored on the server:

- URL queried by the corporate LAN computer, or the domain name from the DNS request.
- URL extracted from the email message prior to normalization.
- IP address of the data packet sender.
- IP address of the data packet recipient.
- Category of the detected object (for example, malicious or phishing URL), and the alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this event may have on computer security or corporate LAN security based on Kaspersky Lab experience.
- VIP group affiliation.
- Information about the proxy server.
- Unique ID of the email message.
- Email addresses of the sender and recipients of the message (including the recipients of copies and blind carbon copies of the message).
- Subject of the email message.
- Date and time when the message was received by Kaspersky Anti Targeted Attack Platform, with precision up to the second.
- List of detected objects.
- Time of network connection.
- URL of network connection.

If the alert was generated by Intrusion Detection System technology, the following information may be stored on the server:

- IDS rule ID.
- Category of the detected object based on the Intrusion Detection System database version.
- Category of the detected object according to the Kaspersky Lab classification.
- Version of the Intrusion Detection System databases used to generate the alert.
- Alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer security or corporate LAN security based on Kaspersky Lab experience.
- File containing the traffic where the alert occurred.
- URL extracted from the file containing the traffic, User Agent, and method.
- IP address and type of integration of the server on which the alert was generated.
- VIP group affiliation.

- Data transfer time.
- IP address of the data packet sender.
- IP address of the data packet recipient.

If the alert was generated using YARA rules, the following information may be stored on the server:

- Version of the YARA rules used to generate the alert.
- Category of the detected object.
- Names of detected objects.
- MD5 hashes of detected objects.

If the alert was generated using the Sandbox component, the following information may be stored on the server:

- Time of alert generation.
- Version of the program databases used to generate the alert.
- Category of the detected object.
- Names of detected objects.
- MD5 hashes of detected objects.
- Additional information about the alert.

If the alert was generated as a result of an IOC scan, the following information may be stored on the server:

- Date and time of scan completion.
- IDs of the computers on which the alert was generated.
- Name of the IOC file.
- Contents of the IOC file.
- Information about detected objects.

Data in events

Events may contain user data. Information about events that have occurred is stored for 30 days on the server with the Central Node component in the directory `/data/var/lib/kaspersky/storage/fastsearch/elasticsearch/data/`.

Kaspersky Anti Targeted Attack Platform resources provide no capability to restrict the rights of the users of servers and operating systems to which the Central Node component is installed. The administrator is advised to use any system resources at their own discretion to control how the users of servers and operating systems with the program installed may be granted access to the personal data of other users.

Event data may contain the following information:

- Name of the computer where the event occurred.
- Name of the user account under which the event occurred.
- Unique ID of the computer with the Endpoint Sensors component.

- Event type.
- Event time.
- Full paths to files on computers with the Endpoint Sensors component.
- Names of files on computers with the Endpoint Sensors component.
- Full names of folders on computers with the Endpoint Sensors component.
- MD5- and SHA256 hash of files.
- File creation time.
- File modification time.
- Command-line parameters.
- Local IP address of the adapter.
- Local port.
- Remote host name.
- Remote host IP address.
- Port on the remote host.
- URLs and IP addresses of visited websites, and links from these websites.
- Path to keys in the Windows registry.
- Information about Windows registry variables: path to the variable, variable name, variable value.
- Details of the process file: path to the file, full name of the file, file size, file creation date, file modification date, MD5- and SHA256 hash of the file.
- Details of the parent process file: full name of the file, path to the file, unique ID of the file, MD5- and SHA256 hash of the file, ID of the Windows parent process.
- Information about the interpreted file: full name of the file, path to the file, MD5- and SHA256 hash of the file.
- Information about the file blocked from starting: full name of the file, path to the file, MD5- and SHA256 hash of the file.
- Information about the DLL module: full name, path, size, DLL module creation date and modification date, MD5- and SHA256 hash of the DLL module.
- Information related to the file creation event: full name of the created file, path, size, creation date and modification date, MD5- and SHA256 hash of the file.
- Information about the driver file: full name of the file, path to the file, size, creation date and modification date, MD5- and SHA256 hash of the file.
- New name and old name of the host, if the host name was changed.
- Name of the detected object.
- Information about the event in the Windows log: event type, event type ID, event ID, user account under which the event was logged, full text of the event from the Windows Event Log in XML format.
- Information related to the KES alert: full name of the detected object, MD5- and SHA256 hash of the file, unique ID of the process, Windows PID, command line parameters, type of detected object, threat name, record ID in the KES database, version of the KES database, scan mode, scan result, reason why the object cannot be disinfected.

Targeted Attack Analyzer data

Alerts may contain user data. Information about alerts generated using Targeted Attack Analyzer technology is stored indefinitely on the server with the Central Node component in the directory `/data/var/lib/kaspersky/storage/fastsearch/detector/data/`. Files whose scan results generated an alert are accumulated on the server hosting the Central Node component and rotated as disk space is filled up.

Kaspersky Anti Targeted Attack Platform resources provide no capability to restrict the rights of the users of servers and operating systems to which the Central Node component is installed. The administrator is advised to use any system resources at their own discretion to control how the users of servers and operating systems with the program installed may be granted access to the personal data of other users.

If the alert was generated by Targeted Attack Analyzer, Backup may contain the following information:

- Host name.
- User name.
- Time of alert generation.
- Name of the detected object.
- Full name and path to the file in which the object was detected.
- MD5- and SHA256 hash of the file.
- VHS of the file.
- File description.
- File creation time.
- File modification time.
- Company that released the program associated with the file.
- File version.
- File author.
- Command-line parameters.
- Name, owner of the domain, date of domain registration, and name of the organization that registered the domain.
- Popularity of the domain throughout the world.
- Date and time of host detection.
- Number of queries to the host.
- Volume of data downloaded from the LAN computer to this host.
- IP address, host name, and port from which data was sent.
- Local IP address and port of the network adapter.
- Version of the program databases used to generate the alert.
- URLs of visited websites.
- Alert type and description.

- Details of the process file: path to the process file, company that released the program linked to the process; program version; file size and version, MD5- and SHA256 hash of the file; author of the certificate containing the digital signature for the detected file, and the validity of the signature.
- Date and time when the process was detected in the local network.
- Number of times the process was detected in the local network.
- Number of computers on which a similar process was detected.
- Global popularity of the file that started the process.
- Global popularity of the path by which the process was loaded.
- Names of DLL libraries that Kaspersky Anti Targeted Attack Platform users are advised to direct their attention, and the DLL activity log.
- Account type, type of login to the computer; date and time when the account was first detected in the local area network; date and time when the account was first detected on the computer; number of computers on which the account was detected.
- Log of HTTP requests and responses for detected processes and domains: every hour, data on each process-domain pair (time, remote host, process file path, number of requests, volume of requests, volume of responses); for each hour, a precise log (individual HTTP requests and responses, IP address and port of the source; IP address, port, and name of the recipient, length of the body and header of the request, length of the body and header of the response, time of the request, URI, remote host name, User Agent, and method); header and body of the request and response for the specific request-response pair.
- Process Activity log for processes involved in the alert: every hour, data on the number of starts per hour for each of the processes listed in the **Processes** section; for each hour, information about the time of each start and the associated command; for each start, the path to the file, MD5- and SHA256 hash of the file; path to the parent file, MD5- and SHA256 hash of the parent file, name, role and domain of the account, type of login to the computer, command, and the process start and termination time.
- Information about the alert.
- VIP group affiliation.
- Unique ID of the computer on which the alert was generated.
- DNS request and response to it.

Data in reports

Reports may contain user data. Information about reports is stored indefinitely on the server with the Central Node component in the directory `/data/var/lib/kaspersky/storage/pgsql/10/data/`.

Kaspersky Anti Targeted Attack Platform resources provide no capability to restrict the rights of the users of servers and operating systems to which the Central Node component is installed. The administrator is advised to use any system resources at their own discretion to control how the users of servers and operating systems with the program installed may be granted access to the personal data of other users.

Reports may contain the following information:

- Report creation date.
- Time period covered in the report.
- Report status.
- Text of the report as HTML code.

Data on objects in Backup

Objects in Backup may contain user data. Information about objects in Backup is stored indefinitely on the server with the Central Node component in the directory `/data/var/lib/kaspersky/storage/pgsql/10/data/`.

Kaspersky Anti Targeted Attack Platform resources provide no capability to restrict the rights of the users of servers and operating systems to which the Central Node component is installed. The administrator is advised to use any system resources at their own discretion to control how the users of servers and operating systems with the program installed may be granted access to the personal data of other users.

Data on objects in Backup may contain the following information:

- Name of the object in Backup.
- Path to the object placed in Backup on the computer with the Endpoint Sensors component.
- MD5- and SHA256 hash of the file.
- ID of the user who placed the object in Backup.
- Unique ID of the computer on which the object is stored in Backup.
- Category of the detected object.
- Object scan results using individual modules and technologies.

Data on program settings

The values of program settings are stored indefinitely on the server with the Central Node component in the directory `/data/var/lib/kaspersky/storage/pgsql/10/data/`.

Kaspersky Anti Targeted Attack Platform resources provide no capability to restrict the rights of the users of servers and operating systems to which the Central Node component is installed. The administrator is advised to use any system resources at their own discretion to control how the users of servers and operating systems with the program installed may be granted access to the personal data of other users.

Data on policies and tasks are stored on the Central Node server in non-encrypted form.

Data on policies

Policy data may contain the following information:

- MD5-, SHA256 hash of the file that is prevented from running.

- Comment.
- Hosts on which the file is prevented from running.
- Status of the prevention.

Data on tasks

Based on the task results, a report is generated that is stored on the server hosting the Central Node component.

Task data may contain the following information:

- Task ID.
- Task creation time.
- Name and IP address of the host to which the task is assigned.
- Maximum task execution time.
- Task priority.
- Path to the file (for file download and deletion tasks, file placement in Storage, process termination).
- On whose behalf it is required to run the program.
- Task type (command execution or file run).
- Path to the file, arguments or command line.
- Working directory.
- Path to the registry key.
- Task report.
- User comments on the task.
- ID of the user account that created the task.

Data on user accounts

Program user account data may contain the following information:

- User ID.
- User account name and password.
- User role in the program.
- Information about user activity.
- Rights to access servers with the PCN role.

Data on Endpoint Sensors components.

Data on Endpoint Sensors components may contain the following information:

- Unique ID of the computer with the Endpoint Sensors component.
- Name of the computer with the Endpoint Sensors component.
- Time when the first packet was received.
- Time when the last packet was received.
- Information about the Self-Defense status.

- Version of the Endpoint Sensors component.
- Time and result of the last IOC scan on the computer with the Endpoint Sensors component.

Data on IOC scan settings.

Data on IOC scan settings may contain the following information:

- Name of the IOC file.
- IOC scan requests.
- Time of last IOC scan completion.
- State of the IOC file.
- Date when the IOC file was loaded.
- Importance level of generated alerts.

Data on network isolation rules.

Data on network isolation rules may contain the following information:

- Rule name.
- Unique ID of the isolated host.
- Rule status.
- Name of the user account that created or modified the rule.
- List of exclusions from the rule.

Data on report templates.

Report template data may contain the following information:

- ID of the user who created or modified the template.
- Template creation date.
- Date of last modification of the template.
- HTML code of the template.

Data on the general settings of the program.

Data on the general settings of the program may contain the following information:

- Settings of layouts in the **Dashboard** section.
- IOC scan settings.
- SIEM system integration settings.
- Mail sensor integration settings.
- Activity indicators of Endpoint Sensors components.
- VIP group addresses.

Service data necessary for program operation

The service data necessary for program operation is provided in the table below. Service data may also contain the user data described above in this section.

Table 7. Service data necessary for program operation

Data type	Storage location	Access to data	Storage duration
Event log of the operating system.	<ul style="list-style-type: none">• /var/log	Access for users with root privileges.	Indefinite.

Data type	Storage location	Access to data	Storage duration
Program data cache (redis).	<ul style="list-style-type: none">• /var/log	User access is defined by the administrator using operating system tools. Access is provided only over an encrypted IPSec channel.	Indefinite.

<p>Alert export files. Files may contain the following information:</p> <ul style="list-style-type: none"> • Name of the computer on which the alert was generated. • Alert time. • Category of the detected object. • IP address of the data packet sender. • IP address of the data packet recipient. • URL of the data packet sender. • URL of the data packet recipient. • UserAgent of the computer with the Endpoint Sensors component. • URL of the visited website. • MD5 hash of the detected object. • SHA256 hash of the detected object. • Full name of the detected object. • Command-line parameters. • Email address of the sender of the message in which the object was detected. • Email addresses of the recipients of the message 	<ul style="list-style-type: none"> • /var/log 	<p>User access is defined by the administrator using operating system tools.</p> <p>Data export is available only for authorized users.</p> <p>Access is provided only over an encrypted IPSec channel.</p>	<p>Indefinite.</p>
--	--	---	--------------------

Data type	Storage location	Access to data	Storage duration
<p>in which the object was detected.</p> <ul style="list-style-type: none"> Name of the domain in which the alert was generated. 			
Artifacts of the Sandbox component, PCAP files of intercepted traffic.	<ul style="list-style-type: none"> /var/opt/kaspersky/apt-agents/sb_storage 	User access is defined by the administrator using operating system tools.	Files are rotated as the allocated storage location is filled.
Object scan queue.	<ul style="list-style-type: none"> /var/opt/kaspersky/apt-collector/spool 	User access is defined by the administrator using operating system tools.	Until scan completion.
Objects in Quarantine, and objects received from the Endpoint Sensors component.	<ul style="list-style-type: none"> /var/opt/kaspersky/apt/edr_quarantine /var/opt/kaspersky/apt/edr_storage 	User access is defined by the administrator using operating system tools.	Files are rotated as the allocated storage location is filled.
YARA rules.	<ul style="list-style-type: none"> /var/opt/kaspersky/apt-agents/yara_rules 	User access is defined by the administrator using operating system tools.	Indefinite.
Certificates of servers used for integration of program components.	<ul style="list-style-type: none"> /etc/ssl/certs 	<p>User access is defined by the administrator using operating system tools.</p> <p>Information about actions with certificates is saved in the program event log.</p>	Indefinite.

Data type	Storage location	Access to data	Storage duration
Encryption keys transmitted between program components.	<ul style="list-style-type: none"> /etc/opt/kaspersky/apt-base/ipsec.d 	<p>User access is defined by the administrator using operating system tools.</p> <p>Information about modifications to encryption keys is saved in the program event log.</p>	Indefinite.

Endpoint Sensors component data

If you are using the Endpoint Sensors component, the files associated with the detected events may be transmitted to the server with the Central Node component.

This data may include personal data of the user or confidential data of your organization.

Transmission of the data from computers with the Endpoint Sensors component to the server with the Central Node component cannot be disabled.

Do not use the Endpoint Sensors component on those computers from which data transfer is forbidden by your corporate policy.

Data received from the Endpoint Sensors component is stored in a database on the server hosting the Central Node component and is rotated as disk space is filled.

Files that are prepared to be sent by the Endpoint Sensors component to the server with the Central Node component are stored on computers hosting the Endpoint Sensors component in open, non-encrypted form in the same folder that is used as the default folder for storing files on each computer with the Endpoint Sensors component prior to sending them.

Files from computers with the Endpoint Sensors component are only sent to the server with the Central Node component via a secure SSL connection (see page [134](#)).

Files that have been encrypted on computers with the Endpoint Sensors component using the Windows Encrypting File System or Kaspersky File Level Encryption (within the program Kaspersky Endpoint Security for Windows) are sent in encrypted form to the server with the Central Node component.

Kaspersky Anti Targeted Attack Platform lets you modify the settings of the local computer hosting the Endpoint Sensors component that impact the performance of the computer during interaction with the Central Node component.

Settings should be modified only when exclusively recommended by Kaspersky Lab Technical Support.

Modifying settings on your own could diminish the performance of the local computer.

The Kaspersky Anti Targeted Attack Platform administrator must independently use the data listed above to ensure the security of computers with the Endpoint Sensors component and Kaspersky Anti Targeted Attack Platform servers. The administrator of Kaspersky Anti Targeted Attack Platform is responsible for access to this information.

This section contains the following information about user data that is stored on computers with the Endpoint Sensors component:

- Contents of stored data
- Storage location
- Storage duration
- User access to data

Data received from the Central Node component

The Endpoint Sensors component saves the values of settings received from the Central Node component on the computer's hard drive. Data is saved in open non-encrypted form in the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\data.

By default, only users with System and Administrator permissions have read-access to files when Self-Defense is enabled. When Self-Defense is disabled, users with System and Administrator permissions can also delete the files, modify their contents, and modify the access rights to them. The Endpoint Sensors component does not manage access rights to this folder and its files. It is the system administrator who determines access permissions.

Data is deleted when the Endpoint Sensors component is removed.

Data received from the Central Node component may contain the following information:

- Data on network connections.
- Data on the operating system that is installed on the server with the Central Node component.
- Data on operating system user accounts.
- Data on user sessions in the operating system.
- Data on Windows event log.
- About a RT_VERSION resource.
- About the contents of a PE file.
- About operating system services.
- Certificate of the server with the Central Node component.
- URL- and IP addresses of visited websites.
- HTTP protocol headers.
- Computer name.

- MD5 hashes of files.
- Unique ID of the computer with the Endpoint Sensors component.
- Names and values of Windows registry keys.
- Paths to Windows registry keys.
- Names of Windows registry variables.
- Name of the local DNS cache entry.
- Address from the local DNS cache entry in IPv4 format.
- IP address or name of the requested host from the local DNS cache.
- Host of the local DNS cache element.
- Domain name of the local DNS cache element.
- Address of the ARP cache element in IPv4 format.
- Physical address of the ARP cache element.
- Serial number of the logical drive.
- Home folder of the local user.
- Name of the user account that started the process.
- Path to the script that is run when the user logs in to the system.
- Name of the user account under which the event occurred.
- Name of the computer where the event occurred.
- Full paths to files on computers with the Endpoint Sensors component.
- Names of files on computers with the Endpoint Sensors component.
- Masks of files on computers with the Endpoint Sensors component.
- Full names of folders on computers with the Endpoint Sensors component.
- Comments of the file publisher.
- Mask of the process file image.
- Path to the process file image that opened the port.
- Name of the process that opened the port.
- Local IP address of the port.
- Trusted public key of the digital signature of executable modules.
- Process name.
- Process segment name.
- Command-line parameters.

Data in logs and trace files

The Endpoint Sensors component can record the component debugging data and the component drivers according to the preset parameters to trace files. By default, the Endpoint Sensors component records no debugging data.

Trace files are never automatically sent outside the confines of the host on which the files were generated. The contents of trace files can be viewed using the standard tools for viewing text files. Trace files are completely deleted when the Endpoint Sensors component is removed.

Trace files are saved in open non-encrypted form in the following folders:

- Trace files of the service portion and drivers of the Endpoint Sensors component are saved in the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\system.

Users with the permissions of the System and Administrator accounts of the operating system can delete the files, modify their contents, and modify access rights to them.

- Trace files of the Shell and graphical interface of the Endpoint Sensors component are saved in the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\user.

Users with the permissions of the User, System and Administrator account of the operating system can delete the files and modify their contents. Users with the permissions of the System and Administrator accounts of the operating system can also modify access rights to the files.

The Endpoint Sensors component does not manage access rights to these folders and to their files. By default, only users with System and Administrator permissions have read-access to files.

Data in trace files may contain the following information:

- Event time.
- Number of thread of execution.
- Program component that caused an alert.
- Event importance.
- Data on executable modules.
- Data on open ports.
- Data on network connections.
- About the operating system that is installed on the computer with the Endpoint Sensors component.
- Data on operating system user accounts.
- Data on user sessions in the operating system.
- Data on Windows event log.
- About alerts of Kaspersky Endpoint Security for Windows.
- About organizational units (OU) of Active Directory®.
- Unique ID of the computer with the Endpoint Sensors component.
- Fully qualified domain name of the computer.
- Serial number of the logical drive.
- HTTP protocol headers.
- Full paths to files on computers with the Endpoint Sensors component.
- Names of files on computers with the Endpoint Sensors component.
- Full names of folders on computers with the Endpoint Sensors component.
- Home folder of the local user.

- Name of the user account that started the process.
- Path to the script that is run when the user logs in to the system.
- Name of the user account under which the event occurred.
- URLs and IP addresses of visited websites, and links from these websites.
- When using a proxy server: Proxy server IP address, computer name, port, proxy server user name.
- External IP addresses, with which a connection was established from a local computer.
- Process start commands.
- Command-line parameters.
- Kaspersky Security Center Network Agent ID.
- Path to keys in the Windows registry.
- Names of Windows registry variables.
- Values of Windows registry variables.
- Windows registry hives.
- Names of detected objects.
- Name of the local DNS cache entry.
- IP address from the local DNS cache entry in IPv4 format.
- IP address or name of the requested host from the local DNS cache.
- Host of the local DNS cache element.
- Domain name of the local DNS cache element.
- IP address of the ARP cache element in IPv4 format.
- Physical address of the ARP cache element.
- Name of the user account that started the operating system service.
- Settings with which the operating system service was started.
- Original name of the file (OriginalFileName) for the RT_VERSION resource.

Data in alerts and events

Event data is saved in binary form in the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata in open non-encrypted form.

By default, only users with System and Administrator permissions have read-access to files when Self-Defense is enabled. When Self-Defense is disabled, users with System and Administrator permissions can also delete the files, modify their contents, and modify the access rights to them. The Endpoint Sensors component does not manage access rights to this folder and its files. It is the system administrator who determines access permissions.

Event data may contain the following information:

- Data on executable modules.
- Data on network connections.
- About the operating system that is installed on the computer with the Endpoint Sensors component.

- Data on user sessions in the operating system.
- Data on operating system user accounts.
- Data on Windows event log.
- About alerts of Kaspersky Endpoint Security for Windows.
- About organizational units (OU) of Active Directory.
- HTTP protocol headers.
- Fully qualified domain name of the computer.
- MD5- and SHA256 hash of files and their fragments.
- Unique ID of the computer with the Endpoint Sensors component.
- Unique IDs of certificates.
- Certificate publisher.
- Certificate subject.
- Name of the algorithm used to generate the certificate fingerprint.
- Address and port of the local network interface.
- Address and port of the remote network interface.
- Program vendor.
- Program name.
- Name of the Windows registry variable.
- Path to the Windows registry key.
- Windows registry variable data.
- Name of the detected object.
- Kaspersky Security Center Network Agent ID.
- Contents of the hosts file.
- Process start command line.

Data contained in task completion reports

Prior to being sent to the Central Node component, the reports and relevant files are temporarily saved on the hard disk drive of the computer with the Endpoint Sensors component. The task completion reports are saved in archived non-encrypted form in the folder `C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\katal\data_queue`.

By default, only users with System and Administrator permissions have read-access to files when Self-Defense is enabled. When Self-Defense is disabled, users with System and Administrator permissions can also delete the files, modify their contents, and modify the access rights to them. The Endpoint Sensors component does not manage access rights to this folder and its files. It is the system administrator who determines access permissions.

Task completion reports contain the following information:

- Data on task output.

- Data on executable modules.
- Data on operating system processes.
- Data on user accounts.
- Data on user sessions.
- Fully qualified domain name of the computer.
- Unique ID of the computer with the Endpoint Sensors component.
- Files of the computer with the Endpoint Sensors component.
- Names of alternate streams of NTFS.
- Full paths to files on the computer with the Endpoint Sensors component.
- Full names of folders on the computer with the Endpoint Sensors component.
- Content of the process standard output.
- Content of the process standard error stream.

Data contained in an install log

The administrator can enable the Endpoint Sensors component install log record (using the `msiexec` standard procedure) during installation using the command line. The administrator shows the path to the file where the install log will be saved.

The log records installation process steps and the `msiexec` command line containing the address of the server hosting the Central Node component and the path to the install log file.

Data on files that are blocked from starting

Data on files that are blocked from starting is stored in open non-encrypted form in the folder `C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata`.

By default, only users with System and Administrator permissions have read-access to files when Self-Defense is enabled. When Self-Defense is disabled, users with System and Administrator permissions can also delete the files, modify their contents, and modify the access rights to them. The Endpoint Sensors component does not manage access rights to this folder and its files. It is the system administrator who determines access permissions.

Data on files that are blocked from starting may contain the following information:

- Full path to the blocked file.
- MD5 hash of the file.
- SHA256 hash of the file.
- Process start command.

Data related to the performance of tasks

When performing a task for placing a file in Quarantine, the archive containing this file is temporarily saved in one of the following folders:

- In the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata\temp for the Endpoint Sensors component that is part of Kaspersky Endpoint Security.
- In the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\data\kata\temp for the Endpoint Sensors component installed from the Kaspersky Anti Targeted Attack Platform package.

When performing a task for running the program on a host, the Endpoint Sensors component locally stores the contents of standard output streams and running process errors in open non-encrypted form until the task completion report is sent to the Central Node component. Files are stored in one of the following folders:

- In the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\kata\temp for the Endpoint Sensors component that is part of Kaspersky Endpoint Security.
- In the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\protected\data\kata\temp for the Endpoint Sensors component installed from the Kaspersky Anti Targeted Attack Platform package.

By default, only users with System and Administrator permissions have read-access to files when Self-Defense is enabled. When Self-Defense is disabled, users with System and Administrator permissions can also delete the files, modify their contents, and modify the access rights to them. The Endpoint Sensors component does not manage access rights to this folder and its files. It is the system administrator who determines access permissions.

Data contained in dump files

When executing a query for providing process dumps, the Endpoint Sensors component locally stores the contents of process dumps in open non-encrypted form in the following folders:

- Dump files of the service portion and drivers of the Endpoint Sensors component are saved in the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\system.

Users with the permissions of the System and Administrator accounts of the operating system can delete the files, modify their contents, and modify access rights to them.

- Dump files and Shell files of the Endpoint Sensors component are saved in the folder C:\ProgramData\Kaspersky Lab\Endpoint Sensor 3.6\logs\user.

Users with the permissions of the User, System and Administrator account of the operating system can delete the files and modify their contents. Users with the permissions of the System and Administrator accounts of the operating system can also modify access rights to the files.

Data is stored until a query execution report is sent to the Central Node component. The Endpoint Sensors component does not manage access rights to this folder and its files. It is the system administrator who determines access permissions. By default, only users with System and Administrator permissions have read-access to files.

Dump files of the Endpoint Sensors component are generated by the operating system during program failures, are stored in the folder specified by operating system settings, and are rewritten upon each failure. Dump files may include any personal data of the user or confidential data of your organization.

Do not use the Endpoint Sensors component on those computers from which data transfer is forbidden by your corporate policy.

Data in dump files may contain the following information:

- Event time.
- Number of thread of execution.

- Program component that caused an alert.
- Event importance.
- Data on executable modules.
- Data on open ports.
- Data on network connections.
- About the operating system that is installed on the computer with the Endpoint Sensors component.
- Data on operating system user accounts.
- Data on user sessions in the operating system.
- Data on Windows event log.
- About alerts of Kaspersky Endpoint Security for Windows.
- About organizational units (OU) of Active Directory.
- Unique ID of the computer with the Endpoint Sensors component.
- Fully qualified domain name of the computer.
- Serial number of the logical drive.
- HTTP protocol headers.
- Full paths to files on the computer with the Endpoint Sensors component.
- Names of files on the computer with the Endpoint Sensors component.
- Full names of folders on the computer with the Endpoint Sensors component.
- Home folder of the local user.
- Name of the user account that started the process.
- Path to the script that is run when the user logs in to the system.
- Name of the user account under which the event occurred.
- URLs and IP addresses of visited websites, and links from these websites.
- When using a proxy server: Proxy server IP address, computer name, port, proxy server user name.
- External IP addresses, with which a connection was established from a local computer.
- Process start commands.
- Command-line parameters.
- Kaspersky Security Center Network Agent ID.
- Path to keys in the Windows registry.
- Names of Windows registry variables.
- Values of Windows registry variables.
- Windows registry hives.
- Names of detected objects.
- Name of the local DNS cache entry.
- Address from the local DNS cache entry in IPv4 format.
- IP address or name of the requested host from the local DNS cache.

- Host of the local DNS cache element.
- Domain name of the local DNS cache element.
- Address of the ARP cache element in IPv4 format.
- Physical address of the ARP cache element.
- Name of the user account that started the operating system service.
- Settings with which the operating system service was started.
- Original name of the file (OriginalFileName) for the RT_VERSION resource.

Sandbox component data

For the processing time, the body of the file sent by the Central Node component is saved in open form on the server hosting the Sandbox component. During processing, the server administrator can access the sent file in Technical Support Mode. The scanned file is deleted by a special script according to the schedule. Once every 60 minutes by default.

Information about the data stored on the server with the Sandbox component is provided in the table below.

Table 8. Data stored on the server with the Sandbox component

Scope of data	Storage location	Storage duration	Access to data
Scanned files	/var/opt/kaspersky/sandbox/library/	After the Central Node component receives the scan results or until automatic deletion, but no more than 24 hours.	User access is defined by the administrator using operating system tools.
File scan results	<ul style="list-style-type: none"> /var/opt/kaspersky/sandbox/library/ /tmp/ 	After the Central Node component receives the scan results or until automatic deletion, but no more than 24 hours.	User access is defined by the administrator using operating system tools.
Settings of tasks	<ul style="list-style-type: none"> /var/opt/kaspersky/sandbox/library/ Sandbox component database 	<p>After the Central Node component receives the scan results or until automatic deletion, but no more than 24 hours in the directory /var/opt/kaspersky/sandbox/library/.</p> <p>Up to 90 days in the Sandbox component database.</p>	<p>User access to the directory /var/opt/kaspersky/sandbox/library/ is defined by the administrator using operating system tools.</p> <p>A password is required for user authentication in the database. Access to database files is granted only to users who started database processes and users with root privileges.</p> <p>Access is provided only over an encrypted IPsec channel.</p>
Trace files	/var/log/kaspersky/sandbox/	Up to 21 days.	<p>User access is defined by the administrator using operating system tools.</p> <p>Only authorized users can perform actions with trace files.</p> <p>Information about actions with trace files is saved in the program event log.</p>

Data transmitted between program components

Central Node and Endpoint Sensors

The Endpoint Sensors component sends to the Central Node component task completion reports, information on events and alerts occurred on computers with the Endpoint Sensors component, and information on termination sessions.

If there is no connection with the Central Node component, all data to be sent is accumulated until it is sent to the Central Node component, or until the Endpoint Sensors component is removed from the computer, but no longer than 21 days.

If an event occurred on the user's computer, the Endpoint Sensors component sends the following data to the events database:

1. File creation event.

- Details of the process that created the file: process file name, and MD5- and SHA256 hash of the process file.
- File name.
- Path to the file.
- Full name of the file.
- MD5- and SHA256 hash of the file.
- Date of file creation and modification.
- File size.
- Event header fields: ProviderName, EventId, Version, Level, Task, Opcode, Keywords, TimeCreatedSystemTime, EventRecordId, CorellationActivityId, ExecutionProcessID, ThreadID, Channel, Computer.
- Event body fields: AccessList, AccessMask, AccountExpires, AllowedToDelegateTo, Application, AuditPolicyChanges, AuthenticationPackageName, CategoryId, CommandLine, DisplayName, Dummy, ElevatedToken, EventCode, EventProcessingFailure, FailureReason, FilterRTID, HandleId, HomeDirectory, HomePath, ImpersonationLevel, IpAddress, IpPort, KeyLength, LayerName, LayerRTID, LmPackageName, LogonGuid, LogonHours, LogonProcessName, LogonType, MandatoryLabel, MemberName, MemberSid, NewProcessId, NewProcessName, NewUacValue, NewValue, NewValueType, ObjectName, ObjectServer, ObjectType, ObjectValueName, OldUacValue, OldValue, OldValueType, OperationType, PackageName, ParentProcessName, PasswordLastSet, PrimaryGroupId, PrivilegeList, ProcessId, ProcessName, ProfileChanged, ProfilePath, Protocol, PublisherId, ResourceAttributes, RestrictedAdminMode, SamAccountName, ScriptPath, ServiceAccount, ServiceFileName, ServiceName, ServiceStartType, ServiceType, SettingType, SettingValue, ShareLocalPath, ShareName, SidHistory, SourceAddress, SourcePort, Status, SubcategoryGuid, SubcategoryId, SubjectDomainName, SubjectLogonId, SubjectUserName, SubjectUserSid, SubStatus, TargetDomainName, TargetLinkedLogonId, TargetLogonId, TargetOutboundDomainName, TargetOutboundUserName, TargetUserName, TargetUserSid, TaskContent, TaskName, TokenElevationType, TransmittedServices, UserAccountControl, UserParameters, UserPrincipalName, UserWorkstations, VirtualAccount, Workstation, WorkstationName.

2. Registry monitoring event.

- Details of the process that modified the registry: Process ID, process file name, and MD5- and SHA256 hash of the process file.
- Path to the registry key.
- Name of the registry variable.
- Registry variable data.

3. Driver loading event.

- File name.
 - Path to the file.
 - Full name of the file.
 - MD5- and SHA256 hash of the file.
 - File size.
 - Date of file creation and modification.
4. Listening port opening event.
- Details of the process that opened the listening port: process file name, and MD5- and SHA256 hash of the process file.
 - Port number.
 - Adapter IP address.
5. Event in the Windows log.
- Time of the event, host on which the event occurred, and user account name.
 - Event ID.
 - Channel/log name.
 - Event ID in the log.
 - Provider name.
 - Authentication event subtype.
 - Domain name.
 - Remote IP address.
6. Process start event.
- Details of the file that started the process: file name, file path, full name of the file, MD5-, SHA256 hash of the file, file size, and date of file creation and modification.
 - UniquePID.
 - Command-line parameters.
 - Details of the parent process: UniquePID, Windows ID of the process, and MD5- and SHA256 hash of the process file.
 - Process termination time.
7. Module loading event.
- Details of the file that loaded the module: UniquePID, file name, file path, full name of the file, MD5- and SHA256 hash of the file, and file size.
 - DLL file name.
 - Path to the DLL file.
 - Full name of the DLL file.
 - MD5- and SHA256 hash of the DLL file.
 - DLL file size.

- Date of DLL file creation and modification.
8. Process startup blocking event.
 - Details of the file that attempted to run: file name, file path, full name of the file, MD5- and SHA256 hash of the file, file size, and date of file creation and modification.
 - Command-line parameters.
 9. File startup blocking event.
 - Details of the file that attempted to open: file name, file path, full name of the file, MD5- and SHA256 hash of the file, type of checksum used for file size blocking ((0 – MD5, !=0 – SHA256, not used for search).
 - Details of the executable file: file name, file path, full name of the file, MD5- and SHA256 hash of the file, file size, and date of file creation and modification.
 - Details of the parent process: file name, file path, full name of the file, MD5- and SHA256 hash of the file, PID, and UniquePID.
 10. Host name change event.
 - Event time.
 - Old host name.
 - New host name.
 11. Hosts file contents modification event.
 - Contents of the hosts file.
 12. Event of Kaspersky Endpoint Security for Windows that is saved in program databases.
 - Information about the Kaspersky Endpoint Security for Windows alert.
 13. Event of Kaspersky Endpoint Security for Windows that is displayed to the user.
 - Scan result.
 - Name of the detected object.
 - ID of the record in program databases.
 - Release time of the program databases with which the alert was generated.
 - Object processing mode.
 - Category of the detected object (for example, name of a virus).
 - MD5 hash of the detected object.
 - SHA256 hash of the detected object.
 - Unique ID of the process.
 - Process PID displayed in the Windows Task Manager.
 - Process run command line.
 - Reason for the error when processing the object.
 14. Active Directory organizational unit (OU) modification event.
 - Information about organizational units (OU) of Active Directory.

Central Node and Sandbox

The Central Node component sends to the Sandbox component files and URLs extracted from the network and email traffic. The files are not changed in any way prior to sending. The Sandbox component sends scan results to the Central Node component.

Central Node and Sensor

The program may transmit the following data between Central Node and Sensor components:

- Files and email messages.
- Data on alerts generated by the Intrusion Detection System and URL Reputation technologies.
- License information.
- White lists.
- Data of the Endpoint Sensors component, if integration with a proxy server (see page [197](#)) has been configured.
- Program databases, if the receipt of database updates from the Central Node component is configured.

Servers with PCN and SCN roles

If the program is running in distributed solution (see page [43](#)) mode, the following data is transmitted between the PCN and connected SCNs:

- Data on alerts.
- Data on events.
- Data on tasks.
- Data on policies.
- Data on IOC scans.
- Data on files in Backup.
- Data on user accounts.
- Data on the license.
- List of computers that have the Endpoint Sensors component installed.
- Objects placed in Backup.
- Files attached to alerts.
- IOC files.

Program licensing


This section covers the main aspects of program licensing.

About the End User License Agreement

The End User License Agreement (EULA) is a binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the program.

Read through the terms of the End User License Agreement carefully before you start using the program.

You can view the terms of the End User License Agreement (EULA) in the following ways:

- During installation of Kaspersky Anti Targeted Attack Platform.
- By reading the text named /EULA/License.<language>.
This file is included in the program distribution kit.
- In the program web interface, in the **Settings** section, **License** subsection, by clicking the **License agreement** button.
- In the web interface of the Sandbox component, in the  menu, by clicking the **End User License Agreement** link.

By confirming that you agree with the End User License Agreement when installing the program, you signify your acceptance of the terms of the EULA. If you do not accept the terms of the End User License Agreement, you must abort program installation and must not use the program.

About the license

The license is a time-limited right to use the program, granted under the End User License Agreement.

A current license entitles you to the following kinds of services:

- Use of the program in accordance with the terms of the End User License Agreement
- Technical support

The scope of services and program usage term depend on the type of license under which the program is activated.

Kaspersky Anti Targeted Attack Platform provides the following types of licenses:

- NFR (not for resale) is a free license for a set period, intended to familiarize the user with the program and to carry out test deployments.
- Commercial—Paid license that is provided when you buy the program.

When the license expires, the program continues to work but with limited functionality (see page [96](#)). To use the program full functionality, you must purchase a commercial license or renew a commercial license.

In the current version of Kaspersky Anti Targeted Attack Platform, the available functionality of the program also depends on the type of key installed.

About the license certificate

The *License Certificate* is a document provided with the key file or activation code.

The License Certificate contains the following license information:

- License key or order number.
- Details of the license holder.
- Information about the program that can be activated using the license.
- Limitation on the number of licensing units (devices on which the program can be used under the license).
- License start date.
- License expiration date or license validity period.
- License type.

About the key

A *license key* is a sequence of bits used to activate and use the program in accordance with the End User License Agreement. A license key is generated by Kaspersky Lab.

► *To add a key to the program,*

download a key file.

Kaspersky Lab can black-list a key over violations of the End User License Agreement. If the key has been black-listed, you have to add a different key to continue using the program.

In the current version of Kaspersky Anti Targeted Attack Platform, the available functionality of the program also depends on the type of key installed:

- **KATA and KEDR keys.** Full functionality of the program.
- **KEDR key.** Receiving and processing of data from network traffic and mail traffic is limited.
- **KATA key.** The web interface sections **Threat Hunting**, **Tasks**, **Prevention**, **IOC Scanner**, **Storage**, and **Endpoint Sensors** have limited functionality.

About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky Lab. Key files are designed to activate the program by adding a key.

After purchasing the program or ordering the trial version of the program, you receive a key file at the email address you specified.

You do not need to connect to Kaspersky Lab activation servers in order to activate the program with a key file.

You can recover a key file if it is accidentally deleted. You may need a key file to register with Kaspersky CompanyAccount.

To restore a key file, contact the vendor of the license.

Viewing information about the license and added keys

In distributed solution (see page [43](#)) and multitenancy mode, you can view information about the license and added keys in the web interface of PCN servers and all connected SCNs under the account of a local administrator, administrator, or users of the program web interface.

► *To view information about the license and added keys,*

In the web interface of the server hosting the Central Node component, select the **Settings** section, **License** subsection.

The web interface shows the following information about the license and added keys:

- License serial number
- Program activation date.
- License expiration date.
- Number of days until license expiration.

During the period within 30 days of license expiration, the **Dashboard** section displays a notification about the need to renew the license. This notification is displayed on all servers with the Central Node component (in distributed solution and multitenancy mode – on PCNs and all connected SCNs) for all users, regardless of their role.

Viewing the text of the End User License Agreement in the web interface of the Central Node

In distributed solution (see page [43](#)) and multitenancy mode, you can view the text of the End User License Agreement in the web interface of PCN servers and all connected SCNs under the account of a local administrator, administrator, or users of the program web interface.

► *To view the text of the End User License Agreement, perform the following steps in the web interface of the server hosting the Central Node component:*

1. Select section **Settings**, subsection **License**.
2. Click the **License agreement** button in the upper-right corner of the workspace.
3. In the opened window, carefully read the text of the End User License Agreement.
4. When you are done, click the **Close** button.

Viewing the text of the Privacy Policy in the web interface of the Central Node

In distributed solution and multitenancy mode, you can view the text of the Privacy Policy in the web interface of PCN servers and all connected SCNs under the account of a local administrator, administrator, or users of the program web interface.

► *To view the text of the Privacy Policy, perform the following steps in the web interface of the server hosting the Central Node component:*

1. Select section **Settings**, subsection **License**.
2. Click the **Privacy Policy** button in the upper-right corner of the workspace.
3. In the opened window, carefully read the text of the Privacy Policy.
4. When you are done, click the **Close** button.

Viewing information about the third-party code used in the program


In distributed solution and multitenancy mode, you can view information about third-party code used in Kaspersky Anti Targeted Attack Platform in the web interface of PCN servers and all connected SCNs under the account of a local administrator, administrator, or users of the program web interface.


► *To view information about third-party code, perform the following steps in the web interface of the server hosting the Central Node component:*

1. Select section **Settings**, subsection **License**.
2. Click the **Third-party code** button in the upper-right corner of the workspace.
3. In the opened window, view the information about third-party code.
4. When you are done, click the **Close** button.

Viewing the text of the End User License Agreement in the web interface of the Sandbox

► *To view the text of the End User License Agreement in the web interface of the server hosting the Sandbox component (see page [166](#)):*

1. Sign in to the Sandbox web interface using the account credentials that you specified during installation of the Sandbox component (see page [102](#)).
2. Click the  button in the lower-left part of the web interface window.
3. This opens a window containing information about the Sandbox component.
4. Click the **End User License Agreement** link to open the window containing the text of the End User License Agreement for the program.

5. Carefully read the text of the End User License Agreement.
6. When you are done, click the  button.

Viewing the text of the End User License Agreement on the computer with the Endpoint Sensors component

On each computer on which a standalone Endpoint Sensors component is installed, the file containing the End User License Agreement of Kaspersky Anti Targeted Attack Platform is located in the EULA folder within the same folder where the Endpoint Sensors component is installed (see page [133](#)).

Adding a key

In distributed solution (see page [43](#)) mode, a key can be added only on the PCN server.

► To add a key:

1. In the window of the program web interface, select the **Settings** section, **License** subsection.
2. Select the type of key: **KATA** or **KEDR**.
3. In the section with the selected key type, click the **Upload** button.

The file selection window opens.

4. Select a key file to download and click the **Open** button.

The file selection window closes.

The key is added to the program.

Replacing a key

In distributed solution (see page [43](#)) mode, a key can be replaced only on the PCN server.

► To replace the active key of the program with a different key:

1. In the window of the program web interface, select the **Settings** section, **License** subsection.
2. Select the type of key: **KATA** or **KEDR**.
3. In the section with the selected key type, click the **Replace** button.

The file selection window opens.

4. Select a key file you want to use to replace the active key and click the **Open** button.

The file selection window closes.

The loaded key will replace the active key of the program.

Removing a key

In distributed solution (see [page 43](#)) mode, a key can be removed only on the PCN server.

► To remove a key:

1. In the window of the program web interface, select the **Settings** section, **License** subsection.
 2. Select the type of key: **KATA** or **KEDR**.
 3. In the section with the selected key type, click **Delete**.
The key removal confirmation window opens.
 4. Click **Yes**.
The key removal confirmation window closes.
- The key is removed.

Program modes based on the license

Kaspersky Anti Targeted Attack Platform provides various operating modes depending on the added keys.

No license

After the program is installed and the web interface is started, the program operates in this mode until you add a key.

Unlicensed mode has the following limitations:

- Program databases are not updated.
- There is no connection to the Kaspersky Security Network Knowledge Base.
- Receiving and processing of data from network traffic and mail traffic is limited.
- The web interface sections **Threat Hunting**, **Tasks**, **Prevention**, **IOC Scanner**, **Storage**, and **Endpoint Sensors** have limited functionality.

Commercial license

In this operating mode, the program connects to the Kaspersky Security Network Knowledge Base and updates its databases.

When the key for commercial license expires, the program stops updating its databases and does not connect to the Knowledge Base of Kaspersky Security Network.

To resume the operation of the program, you must replace the key or add a new commercial license key.

In the current version of Kaspersky Anti Targeted Attack Platform, the available functionality of the program also depends on the type of key installed:

- **KATA and KEDR keys**. Full functionality of the program.
- **KEDR key**. Receiving and processing of data from network traffic and mail traffic is limited.
- **KATA key**. The web interface sections **Threat Hunting**, **Tasks**, **Prevention**, **IOC Scanner**, **Storage**, and **Endpoint Sensors** have limited functionality.

Installing and performing initial configuration of the program

This section contains instructions on installation and initial configuration of the program.

Preparing for installing program components

This section provides information on how to prepare your corporate IT infrastructure for the installation of Kaspersky Anti Targeted Attack Platform components.

Preparing the IT infrastructure for program components installation

► *Before installing the program, prepare your corporate IT infrastructure for the installation of components of Kaspersky Anti Targeted Attack Platform:*

1. Make sure that the servers and the computer intended for managing the web interface of the program, and the computers on which the Endpoint Sensors component is to be installed meet the hardware and software requirements (see page [22](#)).
2. Perform the following preliminary preparations of the corporate IT infrastructure for installation of the Sandbox component:
 - a. For both network interfaces, block access of the server hosting the Sandbox component to the corporate LAN in order to keep the network safe from the objects being analyzed.
 - b. For the first network interface, allow Internet access for the server hosting the Sandbox component for the purposes of database updates and analysis of the behavior of objects.
 - c. For the second network interface, allow inbound connections to the following ports for the server hosting the Sandbox component:
 - TCP 22 for connection to the server over the SSH protocol.
 - TCP 443 for receiving objects to scan from the Central Node component.
 - TCP 8443 for using the program web interface.
3. Perform the following preliminary preparations of the corporate IT infrastructure for installation of the Central Node component:
 - a. Allow inbound connections to the following ports for the server hosting the Central Node component:
 - TCP 22 for connection to the server via SSH.
 - TCP 8081 for receiving data from a server with the Sensor component.
 - TCP 9092 for adding metadata to the Targeted Attack Analyzer database (if the Sensor component is installed on a standalone server).
 - TCP 443 for receiving data from computers with the Endpoint Sensors component.
 - TCP 6379 for synchronization with the Redis database on a server with the Sensor component.
 - TCP 8443 for viewing scan results in the program web interface.
 - b. Allow outbound connections to the following ports for the server hosting the Central Node component:
 - UDP 161 for receiving data on the status of the Sensor component (if the Sensor component is installed on a standalone server).

- TCP 80 and 443 for communication with servers of the KSN service and Kaspersky Lab update servers.
 - TCP 443 for sending objects to the Sandbox component so that they can be scanned.
 - TCP 601 for sending messages to a SIEM system.
 - TCP 13299 for integration with Kaspersky Security Center.
4. Perform the following preliminary preparations of the corporate IT infrastructure for installation of the Sensor component:
- a. For the network interface used for integration with a proxy server and mail server, allow inbound connections to the following ports for the server hosting the Sensor component:
 - TCP 22 for connection to the server via SSH.
 - TCP 1344 for receiving traffic from a proxy server.
 - TCP 25 for receiving SMTP traffic from a mail server.
 - TCP 443 when redirecting traffic from Endpoint Sensors components to the server with the Central Node component.
 - UDP 161 for sending data on the status of components and their databases to the server with the Central Node component.
 - b. Allow outbound connections to the following ports for the server hosting the Sensor component:
 - TCP 8081 for sending objects to the server with the Central Node component.
 - TCP 80 and 443 for communication with servers of the KSN service and Kaspersky Lab update servers.
 - TCP 6379 for synchronization with the Redis database on the server with the Central Node component.
 - TCP 9092 for sending metadata from mirrored traffic to the server with the Central Node component.
 - TCP 995 (or TCP 110 for unprotected connections) for integration with a mail server.

If you install a second network interface that receives only mirrored traffic in a VMware ESXi virtual environment, use the E1000 network adapter or disable the LRO (large receive offload) option on a VMXNET3 network adapter.

5. Allow incoming connections to computers hosting the Endpoint Sensors component and the server hosting the Central Node component directly, without a proxy server.
6. On network equipment, allow an encrypted communication channel between servers that have the Central Node and Sensor components.

The connection between servers that have the Central Node and Sensor components is established within the encrypted communication channel based on IPSec using the ESP protocol.

7. If you are using distributed solution and multitenancy mode, perform the following preliminary preparations of the corporate IT infrastructure for installation of the Central Node components:
 - a. Allow inbound connections to ports 8444 and 5432 for the server with the PCN role.
 - b. Allow inbound connections to port 5432 for the server with the SCN role.

- c. On network equipment, allow the establishment of an encrypted communication channel between servers that have the Central Node and Sensor components.

The connection between servers that have the PCN and SCN role is established within the encrypted communication channel based on IPsec using the ESP protocol.

If needed, you can designate other ports for the program's components to use in the administrator menu of the server with the Central Node component. If you change the ports in the administrator menu, you need to allow connections to these ports in your corporate IT infrastructure.

Preparing the IT infrastructure for integration with a mail server used for receiving messages via POP3

If you are using a Microsoft Exchange mail server as your mail server and an email sender configured a request for read receipt notification, you must disable read receipt notifications. Otherwise, read receipt notifications will be sent from the email address that you have configured as the email address used for receiving messages of Kaspersky Anti Targeted Attack Platform. You must also disable automatic processing of meeting requests to prevent filling of the mailbox used for receiving messages of Kaspersky Anti Targeted Attack Platform.

► *To disable read receipt notifications from the email address used for receiving messages of Kaspersky Anti Targeted Attack Platform:*

1. On the Microsoft Exchange server, check whether or not notifications are enabled. To do so, execute the command:

```
Get-MailboxMessageConfiguration -Identity <email address for receiving
messages by Kaspersky Anti Targeted Attack Platform> | fl
```

2. If notifications are enabled, run the following command:

```
Set-MailboxMessageConfiguration -Identity <email address for receiving
messages by Kaspersky Anti Targeted Attack Platform> -
ReadReceiptResponse NeverSend
```

This will disable read receipt notifications from the email address used for receiving messages of Kaspersky Anti Targeted Attack Platform.

► *To disable automatic processing of meeting requests:*

1. On the Microsoft Exchange server, check whether or not notifications are enabled. To do so, execute the command:

```
Get-CalendarProcessing -Identity <email address for receiving messages
by Kaspersky Anti Targeted Attack Platform> | fl
```

2. If automatic processing of meeting requests is enabled, run the following command:

```
Set-CalendarProcessing -Identity <email address for receiving messages
by Kaspersky Anti Targeted Attack Platform> -AutomateProcessing:None
```

Automatic processing of meeting requests will be disabled.

Preparing the IT infrastructure for integration with a mail server used for receiving messages via SMTP

► *To prepare your corporate IT infrastructure for Kaspersky Anti Targeted Attack Platform integration with a mail server over the SMTP protocol:*

1. On the external mail server, configure rules for forwarding copies of the messages that you want to send for scanning by Kaspersky Anti Targeted Attack Platform to the addresses specified in Kaspersky Anti Targeted Attack Platform.
2. Specify the route for forwarding email messages to the server with the Sensor component.
It is recommended to specify a static route – IP address of the server with the Sensor component.
3. In the firewall of your organization, allow inbound connections to port 25 of the server with the Sensor component from mail servers that are forwarding copies of email messages.

You can also improve the security of Kaspersky Anti Targeted Attack Platform integration with a mail server over the SMTP protocol.

► *To improve the security of Kaspersky Anti Targeted Attack Platform integration with a mail server over the SMTP protocol:*

1. Configure authentication of the Kaspersky Anti Targeted Attack Platform server on the side of the mail servers forwarding email messages for Kaspersky Anti Targeted Attack Platform.
2. Configure mandatory encryption of traffic on mail servers that are forwarding email messages for Kaspersky Anti Targeted Attack Platform.
3. Configure authentication of mail servers forwarding email messages for Kaspersky Anti Targeted Attack Platform on the Kaspersky Anti Targeted Attack Platform side.

Preparing the virtual machine for installing the Sandbox component

► *To prepare the virtual machine for installing the Sandbox component:*

4. Open the virtual machine management console.
5. In the context menu of the virtual machine on which you want to install the Sandbox component, choose **Edit Settings**.
This opens the virtual machine properties window.
6. On the **Virtual Hardware** tab, expand the **CPU** settings group and select the **Expose hardware-assisted virtualization to guest OS** check box.
7. On the **VM Options** tab in the **Latency Sensitivity** drop-down list, select **High**.
8. Click **OK**.

The virtual machine is ready for installing the Sandbox component.

Procedure for installing and configuring program components

Perform the steps for program installation and configuration in the following sequence:

1. Install the disk image containing the Sandbox component.
2. Configure the Sandbox component through the Sandbox web interface.
3. Install the disk images of Microsoft Windows operating systems and software for the Sandbox component.
4. Install the disk image containing the Central Node and Sensor components. Configure the Central Node and Sensor components.

If there are multiple Central Node components, you can use the program in distributed solution and multitenancy mode (see page [43](#)).

If there are multiple Sensor components, you can install and configure the Sensor component (see page [119](#)) on the necessary number of servers.

If you need to use the Central Node component separately from the Sensor component, skip the steps on configuring the Sensor component when installing the Central Node and Sensor components (see page [105](#)).

5. Install the Endpoint Sensors component on computers that belong to the corporate IT infrastructure.

Installing the Sandbox component

This section provides step-by-step instructions on installing the Sandbox component.

► *To begin installation of the Sandbox component,*

run the disk image containing the Sandbox component.

The Setup Wizard starts.

Step 1. Viewing the End User License Agreement and Privacy Policy

To continue installation, please read the End User License Agreement (EULA) and accept its terms. Installation will not continue until you accept the terms of the End User License Agreement.

You also need to read the Privacy Policy and accept its terms.

► *To accept the terms of the End User License Agreement and Privacy Policy:*

1. Select the language for viewing the End User License Agreement and Privacy Policy in the list.
For example, if you want to view the End User License Agreement and Privacy Policy in English, select **English**.
2. Press **ENTER**.
This opens a window showing the End User License Agreement text.
3. Please read the End User License Agreement.
4. If you accept the terms of the End User License Agreement, click the **I accept the terms** button.
This opens a window displaying the text of the Privacy Policy.
5. Please carefully read the Privacy Policy.
6. If you accept the terms of the Privacy Policy, click the **I accept the terms** button.

The Setup Wizard proceeds to the next step.

Step 2. Selecting a disk for installing the Sandbox component

At this step, select a physical disk for installing the Sandbox component.

► *To select a disk for installing the Sandbox component:*

1. In the **Select device** window, in the list of disks, select the disk on which you want to install the Sandbox component.
2. Press **ENTER**.

The archive with the installation files will be unpacked to the disk. The server is restarted.

The Setup Wizard proceeds to the next step.

Step 3. Creating the Sandbox administrator account

At this step, create an administrator account for working in the Sandbox web interface, in the administrator menu and in the management console of the server with the Sandbox component.

► *To create the Sandbox administrator account, proceed as follows:*

1. In the **Username** field, enter the name of the administrator account. The admin account is used by default.
2. In the **Password** field, enter the password for the administrator.

The password must satisfy the following requirements:

- Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
 - Must not be the same as the user name.
3. Enter the password again in the **Confirm password** field.
 4. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 4. Selecting the controlling network interface in the list

To ensure proper functioning of the Sandbox component, you must connect at least two network cards and configure the following network Interfaces:

- Controlling network interface. This interface is intended for providing access to the server with the Sandbox component via the SSH protocol, and the server with the Sandbox component will use this interface to receive objects from the server with the Central Node component.
- Network interface used for Internet access of processed objects. Objects that are processed by the Sandbox component can use this interface to attempt activities on the Internet, and the Sandbox component can analyze their behavior. If you block Internet access, the Sandbox component cannot analyze the behavior of objects on the Internet, and will therefore only analyze the behavior of objects without Internet access.

The network interface used for Internet access of processed objects must be isolated from the local network of your organization.

At this step, select the network interface that you want to use as the controlling interface.

► *To select the controlling network interface:*

1. In the list of network interfaces, select the network interface that you want to use as the controlling interface.
2. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 5. Assigning the address and network mask of the controlling interface

► *To assign the IP address and network mask of the controlling network interface:*

1. In the **Address** field, enter the IP address that you want to assign to this network interface.
2. In the **Netmask** field, enter the network mask in which you want to use this network interface.
3. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 6. Configuring a static network route

► *To configure static network routes, perform the following actions for each network route:*

1. In the **IPv4 Routes** window, select **New**.
2. Press **ENTER**.

This opens the **IPv4 Static Route** window.

3. In the **Address/Mask** field, enter the IP address and mask of the subnet for which you want to configure the network route.
4. In the **Gateway** field, enter the IP address of the gateway.
5. Click **Ok**.

Proceed to configuration of the Sandbox component through the web interface (see page [166](#)).

Installing and configuring the Central Node and Sensor components on the same server

This section provides step-by-step instructions for installing and preconfiguring the Central Node and Sensor components on one server.

If you are installing Kaspersky Anti Targeted Attack Platform in a VMware ESXi hypervisor and are planning to have the program receive mirrored traffic from several virtual networks, you need to preconfigure the ESX server on which you want to install the program.

► *To preconfigure the ESX server, perform the following actions in the VMware ESXi hypervisor:*

1. Start VMware vSphere Client.
2. In the list of ESX servers, select the ESX server that you want to preconfigure.
3. Right-click to open the menu.
4. Select the **Configuration** menu item.
This opens the ESX server reconfiguration window.
5. In the **Hardware** section, select **Networking**.
The settings modification window opens.
6. On the **Ports** tab, select the **VM Network** section.
The **VM Network Properties** window opens.
7. On the **General** tab in the **VLAN ID (Optional)** list, select **All**.
8. Click **Ok**.

The program will be able to receive mirrored traffic from several virtual networks.

Step 1. Starting installation of the Central Node and Sensor components and selecting a server role

► *To begin installing the Central Node and Sensor components and select a server role:*

1. Run the disk image containing the Central Node and Sensor components.
The Setup Wizard starts.
2. Select installation from the **Kaspersky Anti Targeted Attack Platform** installation disk.
The program installation start window opens.
3. Click **OK**.
The server role selection window opens.
4. Select **Act as Central Node**.

The Central Node role includes installation and configuration of the Central Node and Sensor components on the same server.

If you need to use the Central Node component separately from the Sensor component, skip the steps on configuring the Sensor component when installing the Central Node and Sensor components (see page [105](#)).

5. This opens the confirmation window for your server role selection.

Click the **Confirm role** button.

This starts the Wizard for installing the Central Node and Sensor components on the same server.

Step 2. Viewing the End User License Agreement and Privacy Policy

To continue installation, please read the End User License Agreement (EULA) and accept its terms. Installation will not continue until you accept the terms of the End User License Agreement.

You also need to read the Privacy Policy and accept its terms.

► *To accept the terms of the End User License Agreement and Privacy Policy:*

1. Select the language for viewing the End User License Agreement and Privacy Policy in the list.

For example, if you want to view the End User License Agreement and Privacy Policy in English, select **English**.

2. Press **ENTER**.

This opens a window showing the End User License Agreement text.

3. Please read the End User License Agreement.

4. If you accept the terms of the End User License Agreement, click the **I accept the terms** button.

This opens a window displaying the text of the Privacy Policy.

5. Please carefully read the Privacy Policy.

6. If you accept the terms of the Privacy Policy, click the **I accept the terms** button.

The Setup Wizard proceeds to the next step.

Step 3. Selecting a disk for installing the Central Node and Sensor components

► *To select a disk for installing the Central Node and Sensor components:*

1. In the **Select device** window, in the list of disks, select the disk on which you want to install the Central Node and Sensor components.

2. Press **ENTER**.

3. The **Select action** window opens.

4. Select **Install**.

5. Press **ENTER**.

This opens a window displaying a warning that the disk will be formatted.

6. Click the **Install** button.

The disk will be formatted. The server is restarted.

The Setup Wizard proceeds to the next step.

Step 4. Creating an account for working in the administrator menu and in the server management console

► *To create an administrator account for working in the administrator menu and in the server management console:*

1. In the **Username** field, enter the user name for the administrator.
2. In the **Password** field, enter the password for the administrator.

The password must satisfy the following requirements:

- Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
 - Must not be the same as the user name.
3. Enter the password again in the **Confirm password** field.
 4. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 5. Assigning the host name

► *To specify the program host name to be used by DNS servers:*

1. Enter the full domain name of the server into the **Hostname** field.
Specify the server name in FQDN format (for example: host.domain.com or host.domain.subdomain.com).
2. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 6. Enabling a network interface for the first time

Network interfaces must be enabled in order to subsequently configure their settings.

After enabling a network interface for the first time, you will be able to disable and enable each network interface in the network interface configuration window.

► *To enable a network interface for the first time:*

1. In the list of network interfaces, select the network interface that you want to enable.
2. Press **ENTER**.

This opens the confirmation window for enabling the network interface.

3. Click **Yes**.

The network interface will be enabled.

4. Select **Continue**.
5. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 7. Configuring the default network route

During this step, configure the network route that the program will use by default. You can configure the network route using a DHCP server or you can configure a static network route.

Configuring the network route using a DHCP server

► *To configure the network route using a DHCP server:*

1. In the **Default route** list, select **Interface**.
2. Press **ENTER**.
This opens the list of network interfaces.
3. Select the network interface for which you want to configure the network route.
4. Press **ENTER**.
The Setup Wizard returns to the network route configuration window.
The value **dhcp** will be displayed opposite the name of the **Gateway** setting.
5. Select **Continue**.
6. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Configuring a static network route

► *To configure a static network route:*

1. In the **Default route** list, select **Interface**.
2. Press **ENTER**.
This opens the list of network interfaces.
3. Select the network interface for which you want to configure the network route.
4. Press **ENTER**.
The Setup Wizard returns to the network route configuration window.
5. Select the **Gateway** setting.
6. Press **ENTER**.
This opens the confirmation window for the static network route configuration.
7. Click **Yes**.
This opens the window for entering a static gateway address.
8. Enter a static gateway address into the **Gateway** field.

9. Click **Ok**.

The Setup Wizard returns to the network route configuration window.

The static gateway address that you assigned will be displayed opposite the name of the **Gateway** setting.

10. Select **Continue**.

11. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 8. Configuring DNS settings

During this step, configure the DNS settings for the operation of servers with program components. You can configure the assignment of DNS addresses using a DHCP server or you can configure the assignment of static DNS addresses.

Assigning DNS addresses using a DHCP server

You may need to use a DHCP server for assigning DNS addresses if you are configuring Kaspersky Anti Targeted Attack Platform in test mode.

► *To assign DNS addresses using a DHCP server:*

1. In the **Obtain DNS addresses over DHCP** window, select the name of your network interface.
2. Press **ENTER**.
This opens the DNS settings configuration window.
3. Make sure that the values of the **Search list**, **Primary DNS**, and **Secondary DNS** settings are set to **dhcp**.
4. Select **Continue**.
5. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Assigning static DNS addresses

You are advised to assign static DNS addresses if you are not configuring Kaspersky Anti Targeted Attack Platform in test mode.

► *To assign static DNS addresses:*

1. In the **Select action - Resolver** window, select **no**.
2. Press **ENTER**.
This opens the DNS settings configuration window.
3. Select any setting.
For example: **Search list**.
4. Press **ENTER**.
This opens the window for entering static DNS addresses.
5. In the **Search list** field, enter the DNS suffix that you want to use in Kaspersky Anti Targeted Attack Platform.
For example: example.com.
6. In the **Primary** field, enter the IP address of the primary DNS server in IPv4 format.
7. In the **Secondary** field, enter the IP address of the secondary DNS server in IPv4 format.

8. Click **Ok**.

This will open the DNS settings configuration window displaying the assigned static DNS settings.

9. Verify that the DNS settings are correct.
10. Select **Continue**.
11. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 9. Configuring proxy server connection settings

In this step you enable or disable the use of a proxy server for database updates and connecting to the KSN service, configure proxy server connection settings, and enable or disable the use of a proxy server when connecting to addresses in your corporate LAN.

Enabling and disabling the use of a proxy server

► *To enable or disable the use of a proxy server:*

1. Select the **Enabled** setting.
2. Press **ENTER**.

If the use of a proxy server was disabled, it is enabled. The value **yes** will be displayed opposite the name of the **Enabled** setting.

If the use of a proxy server was enabled, it is disabled. The value **no** will be displayed opposite the name of the **Enabled** setting.

Proceed to configuring the proxy server connection settings in the current window.

Configuring proxy server connection settings

► *To configure the proxy server connection settings:*

1. In the **Select Action - Proxy** window, select any parameter.

For example, select the **Host** parameter.

2. Press **ENTER**.

This opens a window for configuring proxy server connection settings.

3. In the **Proxy URL** field, enter the URL of the proxy server, connection port, and the user name and password, if you want to use authentication on the proxy server.

Enter this information in this format: `http://<user name for proxy server>:<password for proxy server>@<IP address or URL of the proxy server>:<port for connecting to the proxy server>`

For example, <http://admin:password@10.1.1.1:3128>

4. Click **Ok**.

This closes the window for configuring proxy server connection settings.

The **Select Action - Proxy** window displays the values of the proxy server connection settings.

Proceed to enabling or disabling the use of a proxy server when connecting to addresses in your corporate LAN in the current window.

If the database update server is inside your corporate IT infrastructure or you use KPSN, disable the use of a proxy server when connecting to addresses in your corporate LAN.

Enabling and disabling the use of a proxy server when connecting to local addresses

► *To enable or disable the use of a proxy server when connecting to addresses in your corporate LAN:*

1. Select the **Local addresses** parameter.
2. Press **ENTER**.

If the use of a proxy server when connecting to addresses in your corporate LAN was disabled, it is enabled. The value **use proxy** will be displayed opposite the name of the **Local addresses** setting.

If the use of a proxy server when connecting to addresses in your corporate LAN was enabled, it is disabled. The value **bypass** will be displayed opposite the name of the **Local addresses** setting.

3. Select **Continue**.
4. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 10. Setting the time zone

► *To set the time zone for Kaspersky Anti Targeted Attack Platform:*

1. In the **Select Timezone - Select Country** window, select a country from the list.
For example, select **Russia**.

2. Press **ENTER**.

This displays a list of time zones available for the selected country.

3. Select a time zone.
4. Press **ENTER**.

This opens a window for confirming the time zone selection.

5. If the time zone has been correctly selected, click **Yes**.

The Setup Wizard proceeds to the next step.

Step 11. Configuring time synchronization with an NTP server

At this step, you can configure the server time synchronization with an NTP server.

► *To disable time synchronization with an NTP server, do the following:*

1. In the **Use NTP to set clock** window, click **No**.
This opens the **Set the system clock manually** window.

2. Click one of the following buttons:

- **No**, if you do not want to set up the time manually.

The Setup Wizard proceeds directly to the next step.

- **Yes**, if you want to set up the time manually.

This opens the **Set the system clock** window where you can define the time settings.

3. Upon finishing with the time settings, select **Continue**.

4. Press **ENTER**.

The Setup Wizard proceeds to the next step.

► *To enable time synchronization with an NTP server, do the following:*

1. In the **Use NTP to set clock** window, click **Yes**.

The **Configure NTP servers** window opens.

2. In the **Configure NTP servers** window, select **New**.

This opens the **Add NTP server** window.

3. In the **NTP server** field, enter the IP address or URL of the NTP, which you want to set the time synchronization with.

4. Click **Ok**.

This closes the **Add NTP server** window.

The address of the NTP server is added to the list of NTP servers in the **Configure NTP servers** window.

5. Select **Continue**.

6. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 12. Connecting to the server with the Sandbox component

► *To connect to the server on which you installed the Sandbox component:*

1. In the **Sandbox access** window, compare the IP address and certificate fingerprint with the IP address and certificate fingerprint on the server hosting the Sandbox component.

2. Select **New**.

3. Press **ENTER**.

4. This opens the **Sandbox Node** window.

5. In the **Sandbox name** field, enter the name of the server with the Sandbox component to be displayed on servers hosting the Central Node component.

6. In the **Sandbox node** field, enter the IP address or URL of the server with the Sandbox component.

7. Click **Ok**.

This opens the **Sandbox Access** window.

8. Check the settings for connecting to the Sandbox server.

9. If you want to enable or disable the use of the server with the Sandbox component, click the line containing the name and address of this server.

If you configured a connection to the server with the Sandbox component, its use is enabled by default.

10. Select **Continue**.

11. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 13. Allocating the disk for the Targeted Attack Analyzer component's database

For optimal performance of the Targeted Attack Analyzer component, it is advised that you allocate on the server a physical disk of at least 1 TB for the component's database.

In this step, you can allocate a physical disk for the Targeted Attack Analyzer component's database or decline allocating a physical disk.

► *To decline disk allocation:*

1. In the **Select device** window, select **Continue without separate disk drive**.
2. Press **ENTER**.

The Setup Wizard proceeds to the next step.

► *To allocate a disk, do the following:*

1. In the **Select device** window, select the disk that you want to allocate for the Targeted Attack Analyzer component's database.
2. Press **ENTER**.

The action confirmation window opens.

3. Click **Yes**.

The server is restarted.

The Setup Wizard proceeds to the next step.

Step 14. Creating a local administrator account for the web interface

► *To create a local administrator account for the program's web interface:*

1. In the **Username** field, enter the user name for the account.
The user name "admin" is used by default.
2. In the **Password** field, enter the password for the administrator.

The password must satisfy the following requirements:

- Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
 - Must not be the same as the user name.
3. Enter the password again in the **Confirm password** field.

4. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 15. Configuring receipt of mirrored traffic from SPAN ports

In this step, you can configure receipt of mirrored traffic from SPAN ports.

- *To give up receipt of mirrored traffic from SPAN ports:*

In the **Enable SPAN traffic processing** window, click **No**.

The Setup Wizard proceeds to the next step.

- *To configure receipt of mirrored traffic from SPAN ports:*

1. In the **Enable SPAN traffic processing** window, click **Yes**.

This opens a window for selecting network interfaces.

By default, receipt of mirrored traffic from SPAN ports is disabled for all interfaces. The value **skip** is displayed to the right of the name of the network interface.

2. Select the network interface from which you want to configure receipt of mirrored traffic.

Do not configure receipt of mirrored traffic from the controlling network interface of the server with the Central Node component.

3. Press **ENTER**.

Receipt of mirrored traffic from SPAN ports on the selected interface is enabled. The value **capture** is displayed to the right of the name of the network interface.

4. If you want to configure receipt of mirrored traffic for other network interfaces, repeat steps 2–3 for each of them.
5. Select **Continue**.
6. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 16. Configuring integration with a proxy server via ICAP

At this step, you can configure Kaspersky Anti Targeted Attack Platform integration with a proxy server in your company, using ICAP.

- *To give up Kaspersky Anti Targeted Attack Platform integration with a proxy server:*

In the **Enable ICAP processing** window, click **No**.

The Setup Wizard proceeds to the next step.

- *To enable Kaspersky Anti Targeted Attack Platform integration with a proxy server:*

1. In the **Enable ICAP processing** window, click **Yes**.

This opens a window showing the URI of the server on which you are installing Central Node.

Use this URI to configure integration with Kaspersky Anti Targeted Attack Platform via ICAP on a proxy server in your company.

2. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 17. Configuring integration with a mail server via POP3

At this step you can configure integration with a mail server via the POP3 protocol after preparing the IT infrastructure of your organization (see page [99](#)).

- *To give up integration with a mail server via POP3:*

In the **Enable POP3 processing** window, click **No**.

The Setup Wizard proceeds to the next step.

- *To configure integration with a mail server via POP3:*

1. In the **Enable POP3 processing** window, click **Yes**.

This opens a window allowing you to configure integration with a mail server via POP3.

2. Select the **Server** setting.

3. Press **ENTER**.

This opens the **POP3 server** window.

4. In the **Server** field, enter the IP address of the mail server with which you need to configure integration.

5. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

6. Select the **Encrypted** setting.

7. Press **ENTER**.

- If the encrypted connection with the mail server has been disabled, it will be re-enabled. The value **yes** will be displayed opposite the name of the **Encrypted** setting.
- If the encrypted connection with the mail server has been enabled, it will be disabled. The value **no** will be displayed opposite the name of the **Encrypted** setting.

8. Select the **Username** setting.

9. Press **ENTER**.

This opens the **POP3 access** window.

10. In the **Username** field, enter the account name to obtain access to the mail server via POP3.

11. In the **Password** field, enter the password to obtain access to the mail server.

12. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

13. Select **Check interval**.

14. Press **ENTER**.

This opens the **Check interval** window.

15. In the **Check interval** field, enter the mail server connection frequency (in seconds).

16. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

17. In the **Accepts certificates** section, configure the settings for TLS encryption of the connection between Kaspersky Anti Targeted Attack Platform and external mail servers over the POP3 protocol.

- If you want the program to accept any TLS certificates when connecting to external mail servers:
 - a. Select the **any certificate** option.
 - b. Press **ENTER** to display the **yes** value opposite the **any certificate** option.
- If you want the program to accept untrusted self-signed TLS certificates when connecting to external mail servers:
 1. Select the **untrusted self-signed** option.
 2. Press **ENTER** to display the **yes** value opposite the **untrusted self-signed** option.
- If you want the program to accept only trusted TLS certificates when connecting to external mail servers:
 - a. Select the **any certificate** option.
 - b. Press **ENTER** to display the **no** value opposite the **any certificate** option.
 - c. Select the **untrusted self-signed** option.
 - d. Press **ENTER** to display the **no** value opposite the **untrusted self-signed** option.

When establishing a connection with an external mail server, it is recommended to configure the acceptance of only trusted TLS certificates. If you accept untrusted TLS certificates, protection of the connection against MITM attacks cannot be guaranteed. Even though the acceptance of trusted TLS certificates also cannot guarantee protection of the connection against MITM attacks, it is the most secure of the supported methods for integration with a mail server over the POP3 protocol.

18. If necessary, in the **Cipher list** section, modify the OpenSSL settings used when establishing a connection with a mail server over the POP3 protocol. Perform the following actions:

- a. Select **edit**.
- b. Press **ENTER**.

The **Cipher list** window opens.

- c. In the **Cipher list** field, modify the set of ciphers.

19. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

20. Select **Continue**.

21. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 18. Configuring integration with a mail server via SMTP

At this step, you can configure integration with a mail server via the SMTP protocol after preparing the IT infrastructure of your organization.

► *To decline integration with a mail server via SMTP:*

In the **Enable SMTP processing** window, click **No**.

The Setup Wizard proceeds to the next step.

► *To configure integration with a mail server via SMTP:*

1. In the **Enable SMTP processing** window, click **Yes**.

This opens a window allowing you to configure integration with a mail server via SMTP.

2. Select the **Clients** setting.
3. Press **ENTER**.

The **Configure Networks** window opens.

4. Select the **New** setting.
5. Press **ENTER**.

6. In the **Network address** field, enter the address of the mail server with which Kaspersky Anti Targeted Attack Platform is allowed to interact over the SMTP protocol.

If you leave the mail server address blank, Kaspersky Anti Targeted Attack Platform will receive messages from all servers.

7. Click **Ok**.
8. Select the **Domains** setting.
9. Press **ENTER**.

The **Configure domains** window opens.

10. Select the **New** setting.
11. Press **ENTER**.

12. In the **Domain** field, enter the name of the mail domain or subdomain to which the mail server administrator needs to configure forwarding of a hidden copy of messages.

If you leave the mail domain name blank, Kaspersky Anti Targeted Attack Platform will receive messages sent to any email address.

13. Click **Ok**.
14. Select the **TLS encryption** setting.
15. Press **ENTER**.

The **Select TLS encryption level** window opens.

16. Select one of the following options for TLS encryption of the connection with the mail server over the SMTP protocol:

- **none**, if you do not want to establish TLS encryption of the connection.
- **optional**, if you want the Kaspersky Anti Targeted Attack Platform server to support TLS encryption of the connection.

- **mandatory**, if you want the Kaspersky Anti Targeted Attack Platform server to require TLS encryption of the connection from the mail server.

17. Press **ENTER**.

18. Select the **Client certs** setting.

19. Press **ENTER**.

The **Select TLS client certificates use** window opens.

20. Select one of the following options for checking the client's TLS certificate when connecting with the mail server over the SMTP protocol:

- **ignore**, if you do not want to check the client's TLS certificate.
- **optional**, if you want the Kaspersky Anti Targeted Attack Platform server to support checking of the client's TLS certificate.
- **mandatory**, if you want the Kaspersky Anti Targeted Attack Platform server to require a TLS certificate from the client.

21. Select the **Message size** setting.

22. Press **ENTER**.

The **Message size limit** window opens.

23. In the **Message size limit** field, specify the maximum size of a received message. The maximum size of a received message must not exceed 10 MB.

24. Click **Ok**.

The Setup Wizard proceeds to the next step.

Installing and configuring the Sensor component on a separate server

This section provides step-by-step instructions for installing and preconfiguring the Sensor component on a separate server.

If you are installing Kaspersky Anti Targeted Attack Platform in a VMware ESXi hypervisor and are planning to have the program receive mirrored traffic from several virtual networks, you need to preconfigure the ESX server on which you want to install the program.

► *To preconfigure the ESX server, perform the following actions in the VMware ESXi hypervisor:*

1. Start VMware vSphere Client.
2. In the list of ESX servers, select the ESX server that you want to preconfigure.
3. Right-click to open the menu.
4. Select the **Configuration** menu item.
This opens the ESX server reconfiguration window.
5. In the **Hardware** section, select **Networking**.
The settings modification window opens.
6. On the **Ports** tab, select the **VM Network** section.
The **VM Network Properties** window opens.
7. On the **General** tab in the **VLAN ID (Optional)** list, select **All**.
8. Click **OK**.

The program will be able to receive mirrored traffic from several virtual networks.

Step 1. Starting installation of the Sensor component and selecting a server role

► *To begin installing the Sensor component and select a server role:*

1. Run the disk image containing the Central Node and Sensor components.
The Setup Wizard starts.
2. Select installation from the **Kaspersky Anti Targeted Attack Platform** installation disk.
The program installation start window opens.
3. Click **OK**.
The server role selection window opens.
4. Select **Act as Sensor**.
This opens the confirmation window for your server role selection.
5. Click the **Confirm role** button.

This starts the Wizard for installing the Sensor component on a separate server.

Step 2. Viewing the End User License Agreement and Privacy Policy

To continue installation, please read the End User License Agreement (EULA) and accept its terms. Installation will not continue until you accept the terms of the End User License Agreement.

You also need to read the Privacy Policy and accept its terms.

► *To accept the terms of the End User License Agreement and Privacy Policy:*

1. Select the language for viewing the End User License Agreement and Privacy Policy in the list.
For example, if you want to view the End User License Agreement and Privacy Policy in English, select **English**.
2. Press **ENTER**.
This opens a window showing the End User License Agreement text.
3. Please read the End User License Agreement.
4. If you accept the terms of the End User License Agreement, click the **I accept the terms** button.
This opens a window displaying the text of the Privacy Policy.
5. Please carefully read the Privacy Policy.
6. If you accept the terms of the Privacy Policy, click the **I accept the terms** button.

The Setup Wizard proceeds to the next step.

Step 3. Selecting a disk for installing the Sensor component

► *To select a disk for installing the Sensor component:*

1. In the **Select device** window, in the list of disks, select the disk on which you want to install the Sensor component.
2. Press **ENTER**.
3. The **Select action** window opens.
4. Select **Install**.
5. Press **ENTER**.
This opens a window displaying a warning that the disk will be formatted.
6. Click the **Install** button.

The disk will be formatted. The server is restarted.

The Setup Wizard proceeds to the next step.

Step 4. Creating an account for working in the administrator menu and in the server management console

► *To create an administrator account for working in the administrator menu and in the server management console:*

1. In the **Username** field, enter the user name for the administrator.
2. In the **Password** field, enter the password for the administrator.

The password must satisfy the following requirements:

- Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
 - Must not be the same as the user name.
3. Enter the password again in the **Confirm password** field.
 4. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 5. Assigning the host name

► *To specify the program host name to be used by DNS servers:*

1. Enter the full domain name of the server into the **Hostname** field.
Specify the server name in FQDN format (for example: host.domain.com or host.domain.subdomain.com).
2. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 6. Enabling a network interface for the first time

Network interfaces must be enabled in order to subsequently configure their settings.

After enabling a network interface for the first time, you will be able to disable and enable each network interface in the network interface configuration window.

► *To enable a network interface for the first time:*

1. In the list of network interfaces, select the network interface that you want to enable.
2. Press **ENTER**.

This opens the confirmation window for enabling the network interface.

3. Click **Yes**.
The network interface will be enabled.
4. Select **Continue**.
5. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 7. Configuring the default network route

During this step, configure the network route that the program will use by default. You can configure the network route using a DHCP server or you can configure a static network route.

Configuring the network route using a DHCP server

► *To configure the network route using a DHCP server:*

1. In the **Default route** list, select **Interface**.
2. Press **ENTER**.
This opens the list of network interfaces.
3. Select the network interface for which you want to configure the network route.
4. Press **ENTER**.
The Setup Wizard returns to the network route configuration window.
The value **dhcp** will be displayed opposite the name of the **Gateway** setting.
5. Select **Continue**.
6. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Configuring a static network route

► *To configure a static network route:*

1. In the **Default route** list, select **Interface**.
2. Press **ENTER**.
This opens the list of network interfaces.
3. Select the network interface for which you want to configure the network route.
4. Press **ENTER**.
The Setup Wizard returns to the network route configuration window.
5. Select the **Gateway** setting.
6. Press **ENTER**.
This opens the confirmation window for the static network route configuration.
7. Click **Yes**.

This opens the window for entering a static gateway address.

8. Enter a static gateway address into the **Gateway** field.
9. Click **Ok**.

The Setup Wizard returns to the network route configuration window.

The static gateway address that you assigned will be displayed opposite the name of the **Gateway** setting.

10. Select **Continue**.
11. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 8. Configuring DNS settings

During this step, configure the DNS settings for the operation of servers with program components. You can configure the assignment of DNS addresses using a DHCP server or you can configure the assignment of static DNS addresses.

Assigning DNS addresses using a DHCP server

You may need to use a DHCP server for assigning DNS addresses if you are configuring Kaspersky Anti Targeted Attack Platform in test mode.

► *To assign DNS addresses using a DHCP server:*

1. In the **Obtain DNS addresses over DHCP** window, select the name of your network interface.
2. Press **ENTER**.
This opens the DNS settings configuration window.
3. Make sure that the values of the **Search list**, **Primary DNS**, and **Secondary DNS** settings are set to **dhcp**.
4. Select **Continue**.
5. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Assigning static DNS addresses

You are advised to assign static DNS addresses if you are not configuring Kaspersky Anti Targeted Attack Platform in test mode.

► *To assign static DNS addresses:*

1. In the **Select action - Resolver** window, select **no**.
2. Press **ENTER**.

This opens the DNS settings configuration window.

3. Select any setting.

For example: **Search list**.

4. Press **ENTER**.

This opens the window for entering static DNS addresses.

5. In the **Search list** field, enter the DNS suffix that you want to use in Kaspersky Anti Targeted Attack Platform.

For example: example.com.

6. In the **Primary** field, enter the IP address of the primary DNS server in IPv4 format.
7. In the **Secondary** field, enter the IP address of the secondary DNS server in IPv4 format.
8. Click **Ok**.

This will open the DNS settings configuration window displaying the assigned static DNS settings.

9. Verify that the DNS settings are correct.
10. Select **Continue**.
11. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 9. Configuring proxy server connection settings

In this step you enable or disable the use of a proxy server for database updates and connecting to the KSN service, configure proxy server connection settings, and enable or disable the use of a proxy server when connecting to addresses in your corporate LAN.

Enabling and disabling the use of a proxy server

► *To enable or disable the use of a proxy server:*

1. Select the **Enabled** setting.
2. Press **ENTER**.

If the use of a proxy server was disabled, it is enabled. The value **yes** will be displayed opposite the name of the **Enabled** setting.

If the use of a proxy server was enabled, it is disabled. The value **no** will be displayed opposite the name of the **Enabled** setting.

Proceed to configuring the proxy server connection settings in the current window.

Configuring proxy server connection settings

► *To configure the proxy server connection settings:*

1. In the **Select Action - Proxy** window, select any parameter.
For example, select the **Host** parameter.
2. Press **ENTER**.

This opens a window for configuring proxy server connection settings.

3. In the **Proxy URL** field, enter the URL of the proxy server, connection port, and the user name and password, if you want to use authentication on the proxy server.

Enter this information in this format: `http://<user name for proxy server>:<password for proxy server>@<IP address or URL of the proxy server>:<port for connecting to the proxy server>`

For example, <http://admin:password@10.1.1.1:3128>

4. Click **Ok**.

This closes the window for configuring proxy server connection settings.

The **Select Action - Proxy** window displays the values of the proxy server connection settings.

Proceed to enabling or disabling the use of a proxy server when connecting to addresses in your corporate LAN in the current window.

If the database update server is inside your corporate IT infrastructure or you use KPSN, disable the use of a proxy server when connecting to addresses in your corporate LAN.

Enabling and disabling the use of a proxy server when connecting to local addresses

► *To enable or disable the use of a proxy server when connecting to addresses in your corporate LAN:*

1. Select the **Local addresses** parameter.
2. Press **ENTER**.

If the use of a proxy server when connecting to addresses in your corporate LAN was disabled, it is enabled. The value **use proxy** will be displayed opposite the name of the **Local addresses** setting.

If the use of a proxy server when connecting to addresses in your corporate LAN was enabled, it is disabled. The value **bypass** will be displayed opposite the name of the **Local addresses** setting.

3. Select **Continue**.
4. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 10. Setting the time zone

► *To set the time zone for Kaspersky Anti Targeted Attack Platform:*

1. In the **Select Timezone - Select Country** window, select a country from the list.

For example, select **Russia**.

2. Press **ENTER**.

This displays a list of time zones available for the selected country.

3. Select a time zone.

4. Press **ENTER**.

This opens a window for confirming the time zone selection.

5. If the time zone has been correctly selected, click **Yes**.

The Setup Wizard proceeds to the next step.

Step 11. Configuring time synchronization with an NTP server

At this step, you can configure the server time synchronization with an NTP server.

► *To disable time synchronization with an NTP server, do the following:*

1. In the **Use NTP to set clock** window, click **No**.
This opens the **Set the system clock manually** window.
2. Click one of the following buttons:
 - **No**, if you do not want to set up the time manually.
The Setup Wizard proceeds directly to the next step.
 - **Yes**, if you want to set up the time manually.
This opens the **Set the system clock** window where you can define the time settings.
3. Upon finishing with the time settings, select **Continue**.
4. Press **ENTER**.

The Setup Wizard proceeds to the next step.

► *To enable time synchronization with an NTP server, do the following:*

1. In the **Use NTP to set clock** window, click **Yes**.
The **Configure NTP servers** window opens.
2. In the **Configure NTP servers** window, select **New**.
This opens the **Add NTP server** window.
3. In the **NTP server** field, enter the IP address or URL of the NTP, which you want to set the time synchronization with.
4. Click **Ok**.
This closes the **Add NTP server** window.
The address of the NTP server is added to the list of NTP servers in the **Configure NTP servers** window.
5. Select **Continue**.
6. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 12. Connecting to the server with the Central Node component

► *To connect to the server on which you installed the Central Node component:*

1. In the **Central Node** field, enter the IP address or URL of the server with the Central Node component.
2. Click **Ok**.

The **Central Node certificate** window opens.

3. Compare the certificate fingerprint with the certificate fingerprint on the server with the Central Node component.
4. If the certificate fingerprints match, click **Accept**.

The **Central Node connection** window opens.

Make sure that the values of the settings for connecting to the Central Node server are correct.

5. Click **Ok**.

To complete the connection of the Sensor component to the server with the Central Node component, you will need to accept the connection request from this Sensor component in the web interface of the server with the Central Node component (see page 214). You can do so at any time, regardless of the progress of installation and configuration of the Sensor component in the Setup Wizard.

The Setup Wizard proceeds to the next step.

Step 13. Selecting the Central Node server as the source of Sensor component database updates

- *To select the Central Node server as the source of Sensor component database updates:*

In the **Update source** window, click **OK**.

The Setup Wizard proceeds to the next step.

Step 14. Configuring receipt of mirrored traffic from SPAN ports

In this step, you can configure receipt of mirrored traffic from SPAN ports.

- *To give up receipt of mirrored traffic from SPAN ports:*

In the **Enable SPAN traffic processing** window, click **No**.

The Setup Wizard proceeds to the next step.

- *To configure receipt of mirrored traffic from SPAN ports:*

1. In the **Enable SPAN traffic processing** window, click **Yes**.

This opens a window for selecting network interfaces.

By default, receipt of mirrored traffic from SPAN ports is disabled for all interfaces. The value **skip** is displayed to the right of the name of the network interface.

2. Select the network interface from which you want to configure receipt of mirrored traffic.

Do not configure receipt of mirrored traffic from the controlling network interface of the server with the Central Node component.

3. Press **ENTER**.

Receipt of mirrored traffic from SPAN ports on the selected interface is enabled. The value **capture** is displayed to the right of the name of the network interface.

4. If you want to configure receipt of mirrored traffic for other network interfaces, repeat steps 2–3 for each of them.
5. Select **Continue**.
6. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 15. Configuring integration with a proxy server via ICAP

At this step, you can configure Kaspersky Anti Targeted Attack Platform integration with a proxy server in your company, using ICAP.

► *To give up Kaspersky Anti Targeted Attack Platform integration with a proxy server:*

In the **Enable ICAP processing** window, click **No**.

The Setup Wizard proceeds to the next step.

► *To enable Kaspersky Anti Targeted Attack Platform integration with a proxy server:*

1. In the **Enable ICAP processing** window, click **Yes**.

This opens a window showing the URI of the server on which you are installing Central Node.

Use this URI to configure integration with Kaspersky Anti Targeted Attack Platform via ICAP on a proxy server in your company.

2. Click **Ok**.

The Setup Wizard proceeds to the next step.

Step 16. Configuring integration with a mail server via POP3

At this step you can configure integration with a mail server via the POP3 protocol after preparing the IT infrastructure of your organization (see page [99](#)).

► *To give up integration with a mail server via POP3:*

In the **Enable POP3 processing** window, click **No**.

The Setup Wizard proceeds to the next step.

► *To configure integration with a mail server via POP3:*

1. In the **Enable POP3 processing** window, click **Yes**.

This opens a window allowing you to configure integration with a mail server via POP3.

2. Select the **Server** setting.
3. Press **ENTER**.

This opens the **POP3 server** window.

4. In the **Server** field, enter the IP address of the mail server with which you need to configure integration.

5. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

6. Select the **Encrypted** setting.

7. Press **ENTER**.

- If the encrypted connection with the mail server has been disabled, it will be re-enabled. The value **yes** will be displayed opposite the name of the **Encrypted** setting.
- If the encrypted connection with the mail server has been enabled, it will be disabled. The value **no** will be displayed opposite the name of the **Encrypted** setting.

8. Select the **Username** setting.

9. Press **ENTER**.

This opens the **POP3 access** window.

10. In the **Username** field, enter the account name to obtain access to the mail server via POP3.

11. In the **Password** field, enter the password to obtain access to the mail server.

12. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

13. Select **Check interval**.

14. Press **ENTER**.

This opens the **Check interval** window.

15. In the **Check interval** field, enter the mail server connection frequency (in seconds).

16. Click **Ok**.

The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.

17. In the **Accepts certificates** section, configure the settings for TLS encryption of the connection between Kaspersky Anti Targeted Attack Platform and external mail servers over the POP3 protocol.

- If you want the program to accept any TLS certificates when connecting to external mail servers:
 - a. Select the **any certificate** option.
 - b. Press **ENTER** to display the **yes** value opposite the **any certificate** option.
- If you want the program to accept untrusted self-signed TLS certificates when connecting to external mail servers:
 1. Select the **untrusted self-signed** option.
 2. Press **ENTER** to display the **yes** value opposite the **untrusted self-signed** option.
- If you want the program to accept only trusted TLS certificates when connecting to external mail servers:
 - a. Select the **any certificate** option.
 - b. Press **ENTER** to display the **no** value opposite the **any certificate** option.
 - c. Select the **untrusted self-signed** option.
 - d. Press **ENTER** to display the **no** value opposite the **untrusted self-signed** option.

When establishing a connection with an external mail server, it is recommended to configure the acceptance of only trusted TLS certificates. If you accept untrusted TLS certificates, protection of the connection against MITM attacks cannot be guaranteed. Even though the acceptance of trusted TLS certificates also cannot guarantee protection of the connection against MITM attacks, it is the most secure of the supported methods for integration with a mail server over the POP3 protocol.

18. If necessary, in the **Cipher list** section, modify the OpenSSL settings used when establishing a connection with a mail server over the POP3 protocol. Perform the following actions:
 - a. Select **edit**.
 - b. Press **ENTER**.
The **Cipher list** window opens.
 - c. In the **Cipher list** field, modify the set of ciphers.
19. Click **Ok**.
The Setup Wizard returns to the window used for configuring integration with a mail server via POP3.
20. Select **Continue**.
21. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 17. Configuring integration with a mail server via SMTP

At this step, you can configure integration with a mail server via the SMTP protocol after preparing the IT infrastructure of your organization.

► *To decline integration with a mail server via SMTP:*

In the **Enable SMTP processing** window, click **No**.

The Setup Wizard proceeds to the next step.

► *To configure integration with a mail server via SMTP:*

1. In the **Enable SMTP processing** window, click **Yes**.
This opens a window allowing you to configure integration with a mail server via SMTP.
2. Select the **Clients** setting.
3. Press **ENTER**.
The **Configure Networks** window opens.
4. Select the **New** setting.
5. Press **ENTER**.
6. In the **Network address** field, enter the address of the mail server with which Kaspersky Anti Targeted Attack Platform is allowed to interact over the SMTP protocol.
If you leave the mail server address blank, Kaspersky Anti Targeted Attack Platform will receive messages from all servers.
7. Click **Ok**.
8. Select the **Domains** setting.
9. Press **ENTER**.
The **Configure domains** window opens.

10. Select the **New** setting.
11. Press **ENTER**.
12. In the **Domain** field, enter the name of the mail domain or subdomain to which the mail server administrator needs to configure forwarding of a hidden copy of messages.
If you leave the mail domain name blank, Kaspersky Anti Targeted Attack Platform will receive messages sent to any email address.
13. Click **Ok**.
14. Select the **TLS encryption** setting.
15. Press **ENTER**.
The **Select TLS encryption level** window opens.
16. Select one of the following options for TLS encryption of the connection with the mail server over the SMTP protocol:
 - **none**, if you do not want to establish TLS encryption of the connection.
 - **optional**, if you want the Kaspersky Anti Targeted Attack Platform server to support TLS encryption of the connection.
 - **mandatory**, if you want the Kaspersky Anti Targeted Attack Platform server to require TLS encryption of the connection from the mail server.
17. Press **ENTER**.
18. Select the **Client certs** setting.
19. Press **ENTER**.
The **Select TLS client certificates use** window opens.
20. Select one of the following options for checking the client's TLS certificate when connecting with the mail server over the SMTP protocol:
 - **ignore**, if you do not want to check the client's TLS certificate.
 - **optional**, if you want the Kaspersky Anti Targeted Attack Platform server to support checking of the client's TLS certificate.
 - **mandatory**, if you want the Kaspersky Anti Targeted Attack Platform server to require a TLS certificate from the client.
21. Select the **Message size** setting.
22. Press **ENTER**.
The **Message size limit** window opens.
23. In the **Message size limit** field, specify the maximum size of a received message. The maximum size of a received message must not exceed 10 MB.
24. Click **Ok**.

The Setup Wizard proceeds to the next step.

Installing and removing the Endpoint Sensors component

This section provides instructions on installing and removing the Endpoint Sensors component.

If you install Kaspersky Endpoint Security on a computer that has the Endpoint Sensor component, the Endpoint Sensor component will be removed regardless of whether or not the Endpoint Sensor component is included in Kaspersky Endpoint Security.

Special considerations for installing the Endpoint Sensors component if the program is used together with KES

Compatibility of KES and Endpoint Sensors component version 3.5

- *If you are using KES version 10 SP2 MR3 or 11.0 and you want to use the standalone Endpoint Sensors component version 3.5:*
1. Disable the Endpoint Sensors component in the KES program.
For more details on how to disable the Endpoint Sensors component in the KES program, refer to the *Kaspersky Endpoint Security Help*.
 2. Install the standalone Endpoint Sensors component version 3.5 on all the computers of your organization's local area network on which you want to use the Endpoint Sensors component.

Compatibility of KES with the standalone Endpoint Sensors component version 3.6

The installation scenario for a standalone Endpoint Sensors component version 3.6 and the KES program on the same computer depends on the version of KES. Information on compatibility of the program and component and installation scenarios are presented in the following table.

KES 11.1 is compatible only with the Endpoint Sensors component included with the KES program. You cannot install KES 11.1 and the standalone Endpoint Sensors component on the same computer.

Table 9. Installation scenarios for KES and the standalone Endpoint Sensors component

Version of KES	Installing the standalone Endpoint Sensors component after installing KES	Installing KES after installing the Endpoint Sensors component
<ul style="list-style-type: none"> • KES10 SP1 MR3 • KES10 SP1 MR4 • KSC 10 SP2 • KSC 10 SP2 MR1 • KSC 10 SP2 MR2 • KSC 10 SP2 MR3 	Standard installation procedure.	Standard installation procedure.
<ul style="list-style-type: none"> • KES 11.0.0 • KES 11.0.1 	<p>You must disable the Endpoint Sensors component included with the KES program.</p> <p>For more details on how to disable the Endpoint Sensors component in the KES program, refer to the <i>Kaspersky Endpoint Security Help</i>.</p> <p>If the component is not disabled, installation fails with an error.</p>	Standard installation procedure.
KES 11.1	Installation fails with an error.	KES removes the standalone Endpoint Sensors component.

Installing the Endpoint Sensors component

Prior to installing the Endpoint Sensors component, the administrator must make sure that the installation folder does not contain files of other applications. It is recommended to grant write-access to the installation folder only to users with the System and Administrator roles.

To be able to install the Endpoint Sensors component, your account must have local administrator privileges.

► To install the Endpoint Sensors component on corporate LAN computers from which Kaspersky Anti Targeted Attack Platform receives and processes data:

1. Use any available method to download the installation file of the Endpoint Sensors component to the computer.
2. Start the command line application on the computer.
3. Type the following command in the command line:

```
msiexec /i "<path to the installation file of the Endpoint Sensors component, including the file name and the msi extension>" /qn /l*v <path to the install log> \install.log SERVER=<address of the server hosting the Central Node component> acceptEULA=1
```

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

4. Press **ENTER**.

Installation of the Endpoint Sensors component finishes.

You can also install the Endpoint Sensors component by using the Microsoft Orca.exe utility or remotely as a Microsoft Windows group policy object. For more details about these installation methods, please refer to Microsoft documentation.

Preparing an SSL connection for data exchange between the Endpoint Sensors and Central Node components

The Endpoint Sensors component continually monitors processes, active network connections, and files that are modified on computers on which the component is installed, and sends this monitoring data to the server with the Central Node component. Based on the results from this data being scanned by the Central Node component, the Endpoint Sensors component can also send files associated with detected events to the server with the Central Node component.

To enable the Endpoint Sensors component to send files to the server with the Central Node component, you need to strengthen the security of the SSL connection between the Endpoint Sensors component and the Central Node server.

You can strengthen the security of the SSL connection between computers with the Endpoint Sensors component and the Central Node server by fulfilling the following conditions when configuring the local network of your organization:

- Deploy Active Directory Domain Services in the local network of your organization.
- Connect the computers on which the Endpoint Sensors component is installed to Active Directory.

Perform the necessary actions to strengthen the security of the SSL connection between computers with the Endpoint Sensors component and the Central Node server in the following sequence:

1. Download the SSL certificate from the server with the Central Node component (see page [134](#)).

You can download a certificate that was automatically created on the server with the Central Node component during the program installation process, a certificate that was manually created on the server with the Central Node component (see page [135](#)), or a certificate that was independently created and uploaded to the server with the Central Node component (see page [135](#)).

2. Prepare an SSL certificate and upload it to Active Directory (see page [137](#)).

Downloading an SSL certificate from the server with the Central Node component

You can download an SSL certificate from the server with the Central Node component to any computer that has access to the server with the Central Node component via the SCP protocol. For more details on the methods for uploading files via the SCP protocol, please refer to the documentation on the operating system installed on the computer to which you want to download the SSL certificate.

- To download the SSL certificate from the server with the Central Node component via the SCP protocol, perform the following actions in your computer's interface used for working over the SCP protocol (using the Linux operating system as an example):

1. Execute the following command: `scp admin@<IP address of the server with the Central Node component>:ssl/kata.crt .`
2. At the password prompt, enter the administrator password for working in the administrator menu of the server with the Central Node component that was set when the Central Node component was installed.

The SSL certificate will be uploaded from the server with the Central Node component to the current folder.

Creating an SSL certificate on the server with the Central Node component

- To create an SSL certificate on the server with the Central Node component, do the following in the administrator menu of the Central Node server (see page [154](#)):

1. In the main window of the administrator menu, select **Program settings**.
2. Press **ENTER**.
3. Select **Manage server certificate**.
4. Press **ENTER**.

This opens the next window of the administrator menu.

5. In the lower part of the window, select **New**.
6. Press **ENTER**.

This opens a window containing information about the new certificate.

7. Click the **Continue** button.

The action confirmation window opens.

8. Click the **Generate** button.

Creation of the certificate starts.

9. After creation of the certificate is completed, press **ENTER**.

This opens a window containing information about the installed certificate.

10. Click the **Continue** button.

The action confirmation window opens.

11. Click **Ok**.

The certificate will be created. The data of previously installed certificates will be overwritten.

Uploading an independently prepared SSL certificate to the server with the Central Node component

You can independently prepare an SSL certificate and upload it to the server with the Central Node component via the SCP protocol. For more details on the methods for uploading files via the SCP protocol, please refer to the documentation on the operating system installed on the computer from which you want to upload the SSL certificate.

The SSL certificate file intended for upload to the server with the Central Node component must satisfy the following requirements:

- The file must contain the certificate itself and a private encryption key for the connection.
- The file must be in PEM format.
- The file name must be `kata.pem`.
- The private key length must be 2048 bits or longer.

For more details on preparing SSL certificates for import, please refer to the documentation on Open SSL.

► *To upload an independently prepared SSL certificate to the server with the Central Node component via the SCP protocol, perform the following actions in your computer's interface used for working over the SCP protocol (using the Linux operating system as an example):*

1. Execute the following command: `scp kata.pem admin@<IP address of the server with the Central Node component>:`
2. At the password prompt, enter the administrator password for working in the administrator menu of the server with the Central Node component that was set when the Central Node component was installed.

The SSL certificate will be uploaded to the server with the Central Node component.

► *To apply the uploaded SSL certificate on the server with the Central Node component, do the following in the administrator menu of the server with the Central Node component (see page [154](#)):*

1. In the main window of the administrator menu, select **Program settings**.
2. Press **ENTER**.

This opens the next window of the administrator menu.

3. Select **Manage server certificate**.
4. Press **ENTER**.

The **Certificate management** window opens.

5. In the lower part of the window, select **kata.pem**.
6. Press **ENTER**.

The **Uploaded certificate** window opens.

7. Select **Install certificate**.
8. Press **ENTER**.

The action confirmation window opens.

9. Click **Yes**.

This opens a window containing information about the certificate.

10. Click the **Continue** button.

The action confirmation window opens.

11. Click the **Install** button.

Installation of the certificate starts.

12. After installation of the certificate is completed, press **ENTER**.

This opens a window containing information about the applied certificate.

13. Click the **Continue** button.

The action confirmation window opens.

14. Click **Ok**.

The certificate will be applied. The data of previously installed certificates will be overwritten.

Preparing and uploading an SSL certificate to Active Directory

- *To prepare and upload an SSL certificate to Active Directory, perform the following actions for each server with the Central Node component:*

1. Select an Active Directory container for the certificate. The Endpoint Sensors component lets you search for the serviceConnectionPoint object in the following locations (in the sequential order of the search):
 - `ldap://CN=<Active Directory Site containing the computer with the Endpoint Sensors component>,CN=Sites,<configurationPartition>`
 - `ldap://CN=Services, <Active Directory configuration partition>`

It is recommended to publish the certificate in the "Sites" container if a separate Central Node component is deployed for any Active Directory Site.

2. In the selected container, create a serviceConnectionPoint object.
3. In a text editor, open the PEM SSL certificate of the server hosting the Central Node component and perform the following actions:
 - a. Delete the strings BEGIN CERTIFICATE and END CERTIFICATE.
 - b. Delete all line breaks.
4. Fill in the attributes of the serviceConnectionPoint as follows:
 - keywords contains the ID string 013D90F9-517B-486D-A7E8-888439D1DD61.
 - serviceDNSName matches the address of the Central Node server specified during installation of the Endpoint Sensors component.
 If an IP address was specified as the address during installation, the attribute must contain the same IP address. If the server FQDN was specified as the address, the attribute must contain the same server FQDN.
 - serviceBindingInformation contains the SSL certificate of the server with the Central Node component in PEM format in one string.

The Endpoint Sensors component performs a sequential search for the serviceConnectionPoint object starting in the Sites container and then in the Services container. It uses the first found object whose keywords attribute contains a unique ID but whose serviceDnsName attribute matches the Central Node server address that was defined during installation of the Endpoint Sensors component.

If the same Active Directory container contains two or more serviceConnectionPoint objects whose keywords attributes contain a unique ID but whose serviceDNSName values match, the Endpoint Sensors component will have limited functionality.

If the Endpoint Sensors component cannot decode the value of the serviceBindingInformation attribute into binary format, or if the attribute value is an empty string, the Endpoint Sensors component will have limited functionality.

Removing the Endpoint Sensors component

To remove the Endpoint Sensors component from a corporate LAN computer, your account must have local administrator privileges.

You can remove the Endpoint Sensors component using the utilities of the Microsoft Windows operating system installed on the corporate LAN computer. The removal procedure depends on the version of the operating system. To learn more about removing programs using the utilities of the Microsoft Windows operating system, please refer to Microsoft documentation.

When the Endpoint Sensors component is removed, the following data is deleted:

- All data accumulated during the operation of the Endpoint Sensors component on the computer.
- Configuration file from the folder C:\Program Data\Kaspersky Lab\Endpoint Sensor 3.6.
- The registry hive HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Endpoint Sensor 3.6\protected (for a 32-bit operating system),
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\Endpoint Sensor 3.6 (for a 64-bit operating system) and all keys stored in it.

After the Endpoint Sensors component is removed, the computer must be restarted.

Configuring traffic redirection from the Endpoint Sensors components to the Sensor component

You can use the server hosting the Sensor component as a proxy server during data exchange between the Endpoint Sensors components and the Central Node component to decrease the burden on the Central Node component.

When configuring the traffic redirection, keep in mind the following limitations:

- The maximum incoming traffic volume for the Sensor component should not exceed 1 Gbit/s.
- The maximum number of computers with the Endpoint Sensors component should be 1,000.
- The recommended channel capacity between servers hosting the Central Node and Sensor components should be 15% of the SPAN port traffic.
- The maximum allowed packet loss between servers hosting the Sensor and Central Node components should be 10% with a packet delay up to 100 ms.

Perform the necessary actions to strengthen the security of the SSL connection of the server hosting the Sensor component with the Central Node server similarly to the actions for the Endpoint Sensors component and the Central Node component in the following sequence:

1. You can use a certificate that was automatically created during the program installation process, a certificate that was manually created on the server with the Sensor component (see page [135](#)), or a certificate that was independently created and uploaded to the server with the Sensor component (see page [135](#)).
2. Prepare an SSL certificate and upload it to Active Directory (see page [137](#)).

You can only use the Sensor component as a proxy server if the Sensor and Central Node components are located on different servers.

If you use the Sensor component as a proxy server, make sure that while configuring the Endpoint Sensors component settings, you entered IP address of the Endpoint Sensors component instead of the Central Node IP address.

Enabling and disabling traffic redirection from the Endpoint Sensors components

- *To enable or disable using the Sensor component as a proxy server for communication between Endpoint Sensors components and the Central Node component, do the following in the administrator menu of the server hosting the Sensor component (see page [154](#)):*

1. In the main window of the administrator menu, select **Program settings**.
2. Press **ENTER**.
This opens the next window of the administrator menu.
3. Select **Configure Central Node**.
4. Press **ENTER**.
5. In the appearing window, enter the IP address of the server hosting the Central Node component.

6. Click **Ok**.

This opens a window containing information on the Central Node component certificate.

7. Make sure that the displayed certificate matches the Central Node component certificate that you downloaded.
8. Click **Accept**.
9. If the connection with the Central Node component is already established, or the request for authorization is sent, click **Yes** in the appearing confirmation window.
10. In the **Update Source** window that opens, perform one of the following actions:
 - If you want to use the server hosting the Central Node component as a source for updating the program databases, click **Yes**.
 - If you do not want to use the server hosting the Central Node component as a source for updating the program databases, click the **No** button.
11. If you want to use the Sensor component as a proxy server, click **Yes** in the **Enable Proxy to Central Node** window that opens.
Using the Sensor component as a proxy server will be enabled after authorization confirmation on the server hosting the Central Node component.
12. If you are already using the Sensor component as a proxy server and want to disable it, click **Yes** in the **Proxy to Central Node** window that opens.
Using the Sensor component as a proxy server will be disabled after authorization confirmation on the server hosting the Central Node component.

Authorizing the Sensor component on a server with the Central Node component

- *To authorize the Sensor component on the server with the Central Node component, do the following in the administrator menu of the Central Node server (see page [154](#)):*

1. In the main window of the administrator menu, select **Program settings**.
2. Press **ENTER**.
This opens the next window of the administrator menu.
3. Select **Configure Sensor Connections**.
This opens a window containing a list of authorization requests from the servers hosting the Sensor component.
4. At the bottom of the window, select the IP address of the server hosting the Sensor component, the request for authorization of which you want to confirm or reject.
The authorization confirmation window opens.
5. If you want to authorize the selected server hosting the Sensor component, select **Accept Sensor**.
The authorization request will be confirmed.
6. If you want to reject authorization of the selected server hosting the Sensor component, select **Reject Sensor**.
The authorization request will be rejected.

Managing Endpoint Sensors components in Kaspersky Security Center.

You can install, remove, and remotely manage Endpoint Sensors components from the Kaspersky Security Center console (hereinafter also referred to as the "KSC Console").

Kaspersky Security Center version 11 also allows using the web console.

For detailed information on working in the KSC Console and web console, see *Kaspersky Security Center Help Guide*.

If you have Endpoint Sensors installed as part of Kaspersky Endpoint Security, you do not have to create an installation package, install or remove the Endpoint Sensors component.

If you install Kaspersky Endpoint Security on a computer that has the Endpoint Sensor component, the Endpoint Sensor component will be removed regardless of whether or not the Endpoint Sensor component is included in Kaspersky Endpoint Security.

For detailed information about installing the Endpoint Sensors component in Kaspersky Endpoint Security, please refer to the *Kaspersky Endpoint Security Help Guide*.

Creating an Endpoint Sensors installation package

To create an installation package, use the Endpoint Sensors component distribution package (the file with the MSI extension included in the distribution kit).

If you have the Endpoint Sensors component installed as part of KES, you do not need to additionally create an installation package and install or remove the Endpoint Sensors component.
For detailed information about installing the Endpoint Sensors component in Kaspersky Endpoint Security, please refer to the *Kaspersky Endpoint Security Help Guide*.

► *To create an installation package for remote installation of the Endpoint Sensors component:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, in the section with additional settings, select the subsection with installation packages.
4. Start the creation of the installation package.

The window of the New Installation Package Wizard opens.

5. If you are using Kaspersky Security Center 10 SP3 or later:
 - a. In the window of the New Installation Package Wizard, select the installation package of the Kaspersky Lab application.

It is not recommended to choose to create an installation package for an external application since in this case, some Endpoint Sensors component remote management features will be unavailable.

- b. Specify the path to the file in KUD format and the name of the new installation package.
- c. Please review the End User License Agreement for this component.

Carefully read the End User License Agreement. If you agree with all of its terms, accept the terms of the End User License Agreement.

Creation of the installation package will then continue. While the installation package is being created, the plug-in for managing the Endpoint Sensors component will be installed in Kaspersky Security Center if you have not already installed it.

- d. Specify the address and port of the server with the Central Node component, as well as the Self-Defense status.

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

Default values: Port 443, server address not defined, Self-Defense enabled.

Self-Defense starts the mechanism for protecting the Endpoint Sensors component against modification or deletion of its files on the drive, memory processes, and system registry entries. To subsequently change the Self-Defense status of the Endpoint Sensors component, you will have to reinstall the component.

- 6. If you are using Kaspersky Security Center 10 SP2 MR1 or 10 SP2, in the window of the New Installation Package Wizard, choose to create an installation package for an external application and specify the following settings in the command line:

- `SELFDEFENSE=On/Off` —Status of Self-Defense.

Self-Defense is enabled by default.

Self-Defense starts the mechanism for protecting the Endpoint Sensors component against modification or deletion of its files on the drive, memory processes, and system registry entries. To subsequently change the Self-Defense status of the Endpoint Sensors component, you will have to reinstall the component.

- `SERVER=<server address>`—Address of the server with the Central Node component.

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

By default, the server address is not defined.

- `acceptEULA=1`—You accept the terms of the End User License Agreement.

You can view the terms of the End User License Agreement by reading the `license.txt` file. This file is included in the program distribution kit. If you agree with all of its terms, accept the End User License Agreement.

- `MESSAGEQUEUEPRINTMESSAGESTOLOG=1`—Log events on the server with the Central Node component.

Optional parameter.

Continual use of event logging can quickly fill up free disk space. Use event logging only when necessary.

You can also enter the following event logging parameters:

- `TRACELEVEL=500` if you want to log errors only.
- `TRACELEVEL=800` if you want to use event logging in debug mode.

For information on configuring additional settings, you can contact Technical Support.

After the wizard finishes, the created installation package will appear in the workspace of the folder containing installation packages.

Remotely installing the Endpoint Sensors component

If you have the Endpoint Sensors component installed as part of KES, you do not need to additionally create an installation package and install or remove the Endpoint Sensors component. For detailed information about installing the Endpoint Sensors component in Kaspersky Endpoint Security, please refer to the *Kaspersky Endpoint Security Help Guide*. Prior to installing a new version of the Endpoint Sensors component, make sure that the local computer has no previous version of this component installed.

You can remotely install the Endpoint Sensors component to a computer using Kaspersky Security Center 11, Kaspersky Security Center 10 SP3, Kaspersky Security Center 10 SP2 MR1, or Kaspersky Security Center 10 SP2.

For detailed information about installing the Endpoint Sensors component in Kaspersky Endpoint Security, please refer to the *Kaspersky Endpoint Security Help Guide*.

► *To remotely install the Endpoint Sensors component to corporate LAN computers:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, select the section containing tasks.
4. In the workspace, select task creation.
The New Task Wizard starts.
5. In the New Task Wizard, choose to create a remote installation task.
6. Select an administration group or individual computers on which you want to install the Endpoint Sensors component.
7. Leave the default settings unchanged.

The New Task Wizard will create a remote installation task. The created task will be placed in the folder containing tasks or will be added to tasks of the administration group for which it was created.

Remotely changing the settings of the Endpoint Sensors component

You can remotely change the settings of the Endpoint Sensors component by reinstalling it on corporate LAN computers.

► *To remotely change the settings of the Endpoint Sensors component on corporate LAN computers:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, in the section with additional settings, select the subsection with installation packages.
4. Start the creation of the installation package.

The window of the New Installation Package Wizard opens.

5. If you are using Kaspersky Security Center 11 or Kaspersky Security Center 10 SP3:
 - a. In the window of the New Installation Package Wizard, select the installation package of the Kaspersky Lab application.
 - b. Specify the path to the file in KUD format and the name of the new installation package.
 - c. Please review the End User License Agreement for this component.

Carefully read the End User License Agreement. If you agree with all of its terms, accept the terms of the End User License Agreement.

Creation of the installation package will then continue. While the installation package is being created, the plug-in for managing the Endpoint Sensors component will be installed in Kaspersky Security Center if you have not already installed it.

- d. Specify the address and port of the server with the Central Node component, as well as the Self-Defense status.

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

Default values: Port 443, server address not defined, Self-Defense enabled.

Self-Defense starts the mechanism for protecting the Endpoint Sensors component against modification or deletion of its files on the drive, memory processes, and system registry entries. To subsequently change the Self-Defense status of the Endpoint Sensors component, you will have to reinstall the component.

6. If you are using Kaspersky Security Center 10 SP2 MR1 or Kaspersky Security Center 10 SP2, in the window of the New Installation Package Wizard choose to create an installation package for an external application and specify the following settings in the command line:
 - `SELFDEFENSE=On/Off` —Status of Self-Defense.

Self-Defense is enabled by default.

Self-Defense starts the mechanism for protecting the Endpoint Sensors component against modification or deletion of its files on the drive, memory processes, and system registry entries. To subsequently change the Self-Defense status of the Endpoint Sensors component, you will have to reinstall the component.

- `SERVER=<server address>`—Address of the server with the Central Node component.

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

By default, the server address is not defined.

- `acceptEULA=1`—You accept the terms of the End User License Agreement.

Carefully read the End User License Agreement. If you agree with all of its terms, accept the terms of the End User License Agreement.

- `MESSAGEQUEUEPRINTMESSAGESTOLOG=1`—Log events on the server with the Central Node component.

Optional parameter.

Continual use of event logging can quickly fill up free disk space. Use event logging only when necessary.

You can also enter the following event logging parameters:

- `TRACELEVEL=500` if you want to log errors only.
- `TRACELEVEL=800` if you want to use event logging in debug mode.

For information on configuring additional settings, you can contact Technical Support.

7. In the workspace, select the installation package of the Endpoint Sensors component.
8. In the section for working with the selected object, start the installation of the program.

The Remote Installation Wizard starts.

9. Select the computers on which you want to install the Endpoint Sensors component.

You can select an administration group or individual devices.

10. Leave the default settings unchanged.

The Wizard will create and start the remote installation task to install the Endpoint Sensors component with the new values of settings. The created task will be placed in the folder containing tasks or will be added to tasks of the administration group for which it was created.

Remotely uninstalling the Endpoint Sensors component

If you have the Endpoint Sensors component installed as part of KES, you do not need to additionally create an installation package and install or remove the Endpoint Sensors component. For detailed information about installing the Endpoint Sensors component in Kaspersky Endpoint Security, please refer to the *Kaspersky Endpoint Security Help Guide*.

You can remotely uninstall the Endpoint Sensors component from a computer using Kaspersky Security Center 11 or Kaspersky Security Center 10 SP3. Remote uninstallation of the Endpoint Sensors component from a computer using Kaspersky Security Center 10 SP2 MR1 or Kaspersky Security Center 10 SP2 is not supported.

► *To remotely uninstall the Endpoint Sensors component from corporate LAN computers:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, select the folder containing tasks.
4. Start the task creation process.
The New Task Wizard window opens.
5. Select the remote uninstallation task.
6. In the list of applications of Kaspersky Security Center, select the Endpoint Sensors component.
7. Select an administration group or set of devices from which you want to remove the Endpoint Sensors component.
8. Specify the task name and start time.

The newly created task is displayed in the workspace of the folder containing tasks. As a result of the remote uninstallation task, the Endpoint Sensors component will be removed from the selected devices.

Remotely starting and stopping the Endpoint Sensors component

You can temporarily disable the Endpoint Sensors component if it hinders the operations of a user, and enable it later. It is not recommended to disable the component for a long time because this reduces corporate LAN security.

► *To start or stop the Endpoint Sensors component on a corporate LAN computer:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, select the device on which you want to stop or start the Endpoint Sensors component.
4. Use the context menu to go to the component properties window.
5. If you want to stop or start an Endpoint Sensors component that is used as part of KES, select the tab containing tasks.
6. If you want to stop or start an Endpoint Sensors component that is not part of KES, select the tab containing apps.

7. On the tab that opens, select the Endpoint Sensors component.
8. Stop or start the Endpoint Sensors component.

After it is stopped, the Endpoint Sensors component will stop monitoring processes, active network connections and files that are modified, and will stop forwarding monitoring data to the server with the Central Node component.

Creating a policy for remote management of the Endpoint Sensors component

You can use Kaspersky Security Center 11 or Kaspersky Security Center 10 SP3 to create a policy for remote management of the Endpoint Sensors component on a computer.

If you have the Endpoint Sensors component installed as part of KES, you do not need to additionally create a policy.

For detailed information about installing the Endpoint Sensors component in Kaspersky Endpoint Security, please refer to the *Kaspersky Endpoint Security Help Guide*.

To work with policies in Kaspersky Security Center, the Endpoint Sensors component administration plug-in must be installed. For detailed information on installing the administration plug-in in Kaspersky Security Center, please refer to the *Kaspersky Security Center Help Guide*.

► To create a policy for remote management of the Endpoint Sensors component:

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, select the section containing policies.
4. Start the New Policy Wizard.

The New Policy Wizard window opens.

5. Specify the policy name.
6. Specify the address and port of the server with the Central Node component.

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

Default values: Port 443, server address not defined.

7. Select the group of computers to which the policy will be applied.
8. Create the new policy as active.

After the wizard finishes, the new policy will be created. The list of all policies is displayed in the policies folder of the KSC console tree.

Reconfiguring a policy for remote management of the Endpoint Sensors component

You can use Kaspersky Security Center 11 or Kaspersky Security Center 10 SP3 to change the settings of a policy for remote management of the Endpoint Sensors component on a computer.

► *To reconfigure a policy for remote management of the Endpoint Sensors component:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, in the section containing policies, select the policy whose settings you want to edit.
4. Use the context menu to go to the policy properties window.
5. Make the relevant changes.

You can change the following:

- Settings for displaying various types of Endpoint Sensors components in the status log.
- Storage period for various types of Endpoint Sensors components in the status log.
- Address and port of the server with the Central Node component.

If you use the Sensor component as a proxy server, enter the IP address or FQDN of the server hosting the Sensor component instead of the Central Node IP address or FQDN.

6. Apply the changes.

Changes to the policy will be saved.

Receiving data from the Endpoint Sensors component in the Kaspersky Security Center Administration Console

You can receive data on the status of the Endpoint Sensors component from the Kaspersky Security Center Administration Console.

For detailed information on working in the KSC Console, please refer to the *Kaspersky Security Center Help Guide*.

Creating a selection of computers based on the presence or properties of Endpoint Sensors components

► *To create a selection of computers based on the properties of Endpoint Sensors components or the presence of Endpoint Sensors components on the computers:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, in the section for selecting devices, create a new selection.
4. In the properties of the selection, add the condition created by default.
5. Open the properties of the new condition.
6. Use tags to add to the default condition according to the desired result. You can also move to other sections for additional actions to search for necessary information on Endpoint Sensors components.

For example, if you want to receive a list of computers on which the Endpoint Sensors component is stopped, in the component status section add the regular expression `KATA:server address*` and the `Stopped` status of the Endpoint Sensors component to the default condition.

Table 10. Settings for creating a selection of computers with the Endpoint Sensors component

List of computers on which...	Regular expression	Necessary action	Additional actions
...the Endpoint Sensors component is installed.	KATA: *	Include	No value.
...the Endpoint Sensors component is not installed.	KATA: *	Exclude	No value.
...the Endpoint Sensors component is installed and configured to connect with any Central Node component.	KATA: server address*	Include	No value.
...the Endpoint Sensors component is installed and configured to connect with a specific Central Node component.	KATA: server address:<server name>:443	Include	No value.
...a specific version of the Endpoint Sensors component is installed.	No value	No value	In the new condition, in the section with the names of applications, select the Endpoint Sensors component and specify the version number.
...the Endpoint Sensors component is installed as part of a specific version of KES.	KATA: agent version:<version number>	Include	No value.
...KES is installed but Endpoint Sensors is not part of KES.	KATA: *	Exclude	In the section with the names of applications, select Kaspersky Endpoint Security.
...the Endpoint Sensors component is installed as part of KES, but is not enabled.	KATA: agent version*	Include	No value.
	KATA: server address*	Exclude	No value.

List of computers on which...	Regular expression	Necessary action	Additional actions
...the Endpoint Sensors component is stopped.	KATA:server address*	Include	In the component status section, add the following status of the Endpoint Sensors component to the condition: Stopped.
...the Endpoint Sensors component is installed but there is no connection with the Central Node component.	No value	No value	In the component status section, add the following status of the Endpoint Sensors component to the condition: Connection to server is failed.
			In the component status section, add the following status of Kaspersky Endpoint Security 11 to the condition: Connection to server is failed.
...the Endpoint Sensors component is installed but is not performing tasks.	No value	No value	In the component status section, add the following status of the Endpoint Sensors component to the condition: Tasks don't work.
			In the component status section, add the following status of Kaspersky Endpoint Security to the condition: Tasks don't work.
...Self-Defense of the Endpoint Sensors component is disabled.	No value	No value	In the component status description section, select the following value for the Endpoint Sensors component status: Self-defense is off.

Receiving data on the status of the Endpoint Sensors component on a specific computer

► *To receive data on the status of the Endpoint Sensors component on a specific computer:*

1. Open the KSC Console.
2. Select the relevant Administration Server.
3. In the KSC console tree, in the section with managed devices, select the relevant computer.

The workspace will display data on the current status of the Endpoint Sensors component on this computer.

4. Select the tab containing events in the computer properties.

The event log opens. Events related to the operation of the Endpoint Sensors component contain the "Endpoint Sensor" string in the tasks column.

Getting started with the program

This section contains information about how to begin working with the program in the web interface, in the administrator menu, and in Technical Support Mode.

Getting started with the program web interface

The web interface of Kaspersky Anti Targeted Attack Platform is hosted by the server with the Central Node component.

The web interface of Kaspersky Anti Targeted Attack Platform is protected against *CSRF attacks* and operates only if the program web interface user's browser provides the Referrer header of an HTTP POST request. Make sure that the browser that you are using to work with the Kaspersky Anti Targeted Attack Platform web interface does not modify the Referrer header of an HTTP POST request. If the connection with the web interface of Kaspersky Anti Targeted Attack Platform is established through a proxy server of your organization, make sure that the proxy server does not modify the Referrer header of an HTTP POST request.

► To begin working with the web interface:

1. In a browser on any computer on which access to the Central Node server has been allowed, enter the IP address of the server with the Central Node component.

An input window for account credentials of the Kaspersky Anti Targeted Attack Platform user opens.

2. Enter the user name and password that you specified during installation and configuration of the Central Node component to access the program web interface.

The **Dashboard** page of the program web interface opens.

You can start using the Kaspersky Anti Targeted Attack Platform web interface.

Getting started with the program administrator menu

You can work with the settings of each of the program's Sensor, Central Node and Sandbox components in the administrator menu in the management console of each server on which the program component is installed.

► To start working in the Sandbox, Sensor or Central Node component administrator menu in the management console of a server hosting the Sandbox, Sensor or Central Node component, proceed as follows:

1. Sign in to the management console of the server whose settings you want to change via the SSH protocol or through a terminal.
2. When the system prompts you, enter the administrator's user name and the password that was specified during program installation (see page [97](#)).

The program component administrator menu is displayed.

You can begin working in the program component administrator menu.

Getting started with the program in Technical Support Mode

You are advised not to perform any actions with Kaspersky Anti Targeted Attack Platform in Technical Support Mode without consultations with or instructions from Technical Support staff.

You can work with the Sensor, Central Node and Sandbox components of the program in Technical Support Mode.

Technical Support Mode provides the Kaspersky Anti Targeted Attack Platform administrator with unrestricted access rights (root) to the program and all of its stored data (including personal information).

Working with Kaspersky Anti Targeted Attack Platform from the management console in Technical Support Mode (see page [155](#)) with superuser account rights enables you to:

- Manage program operation settings using configuration files.

You can also modify the settings for data encryption when data is transferred between program nodes, and the settings for storing and processing objects being scanned.

In this case, data is transmitted in unencrypted form. The Kaspersky Anti Targeted Attack Platform administrator must use this data independently to ensure protection of servers. The Kaspersky Anti Targeted Attack Platform administrator is responsible for modifying the configuration files of the program.

- Manage trace log settings.

Trace files may contain confidential data of the user.

► To start using the program in Technical Support Mode:

1. Sign in to the management console of the server whose settings you want to change via the SSH protocol or through a terminal.
2. When the system prompts you, enter the administrator's user name and the password that was specified during program installation (see page [97](#)).

The program component administrator menu is displayed.

3. In the program administrator menu, select **Technical Support Mode**.
4. Press **ENTER**.

The Technical Support Mode confirmation window opens.

5. If you are sure you would like to work with the program in Technical Support Mode, select **Yes** and press **ENTER**.

Managing accounts of program administrators and users

Kaspersky Anti Targeted Attack Platform provides accounts for servers with the following components:

- **Sensor.** Administrator account for working in the program administrator menu and in the server management console (in Technical Support Mode).
The admin account is used by default.
- **Sandbox.** Administrator account for working in the program administrator menu, in the server management console (in Technical Support Mode) and in the Sandbox web interface.
The admin account is used by default.
- **Central Node.** The following accounts:
 - Administrator account for working in the program administrator menu and in the server management console (in Technical Support Mode).
The admin account that was created during program installation is used by default.
 - Local administrator account of the program web interface.
The Administrator account that was created during program installation is used by default. You can create other administrator accounts for the program web interface (see page [158](#)) after installation.
 - Administrator account of the program web interface.
 - Program web interface user accounts with the **Security officer** and **Senior security officer** roles.

Data from each of these accounts is stored on the server hosting the program component to which the account belongs.

In distributed solution (see page [43](#)) and multitenancy mode, data from each of these accounts is stored on the PCN and on the server hosting the program component to which the account belongs.

The administrator account used for working in the server management console has unlimited rights to manage the server hosting the program component to which the account belongs (superuser rights). Under this account, you can turn off or restart a server, or modify the settings of the program in Technical Support Mode in the server management console.

An administrator account for working in the management console of a server (admin) has unlimited access to data on that server. The password of the administrator account for working in the server management console must be strong. The administrator must independently ensure the security of the server. The administrator bears responsibility for access to data stored on servers.

An account with the **Administrator** role can add, enable and disable program user accounts, and change the passwords of program administrator accounts and web interface user accounts. In distributed solution (see page [43](#)) and multitenancy mode, user accounts are managed on the PCN.

The local administrator account of the program web interface is intended for employees of your organization who need to manage Kaspersky Anti Targeted Attack Platform. When signing in to the program under this account, you will see all sections of the web interface that are available to a user with the **Administrator** role (see page [179](#)).

The administrator account of the program web interface allows to manage the program, however, unlike the local administrator account of the program web interface, such accounts are not allowed to manage PCN and SCN servers or organizations in the **Operation mode** section.

The **Security officer** and **Senior security officer** roles are intended for employees of your organization who are tasked with working with events and tasks of Kaspersky Anti Targeted Attack Platform. When signing in to the program under accounts with these roles, you will see all sections of the web interface that are available to security officers (see page [229](#)). All operations are available to users with the **Senior security officer** role. The restrictions of users with the **Security officer** role are presented in the table below.

Table 11. Access restrictions of program users with the **Security officer** role

Functional scope / Section of the web interface	Restrictions
Dashboard	Widgets of VIP group events are not available. It is not possible to use a link on the widget to go to the Alerts section.
Alerts	The following actions are not available: <ul style="list-style-type: none"> • Viewing information about an alert. • Marking the completion of VIP group alert processing. • Performing operations on multiple alerts. • Exporting the list of all alerts.
Threat Hunting	Events that are associated with hosts from VIP group alerts are not available.
Tasks	No access.
Prevention	No access.
IOC/IOA Analysis	Read access.
Storage	There is no access to objects that are placed in Storage as a result of tasks. Full access to objects that were manually downloaded by the user.
Endpoint Sensors	Access to view tables of computers with the Endpoint Sensors component, and restrictions on viewing data on tasks, policies, and network isolation.
Network isolation of hosts	No access.
Reports	No access.
Settings: IOC scanning schedule	Read access.

Functional scope / Section of the web interface	Restrictions
Settings: Endpoint Sensors	Read access.
Settings: KPSN rules	No access.
Settings: Notifications	No access to rules for sending notifications about alerts. Full access to rules for sending notifications about problems in program operation.
Settings: VIP Status	Read access.
Settings: YARA Rules	Access only to export rules.
Settings: White List	Access to read and export.
Settings: Passwords to archives	No access.
Settings: License	Read access.

If you are using distributed solution and multitenancy mode, access to organizations and web interface of the SCN server can be allowed or blocked for each account.

Creating an administrator account for the program web interface

The administrator account of the program web interface allows to manage the program, however, unlike the local administrator account of the program web interface, such accounts are not allowed to manage PCN and SCN servers or organizations in the **Operation mode** section.

► *To create an administrator account for the program's web interface:*

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Click the **Add** button.

This opens the **New user** window.

4. To enable an account, turn on the **Status** toggle switch.

By default, the account is enabled.

If a user account is enabled, the user is allowed to access the program web interface. If a user account is disabled, the user is prohibited from accessing the program web interface.

5. In the **Role** drop-down list, select **Administrator**.
6. In the **User name** field, enter a user name for the account you want to create.

The user name must meet the following requirements:

- Must be unique in the list of user names (case-sensitive).
- Must contain no more than 32 characters.
- Can contain letters A-Z, a-z, numbers 0-9, hyphens (-), and underscores (_).

- Must begin with a letter (A-Z or a-z).
7. In the **New password** text box, enter a password that will be used to access the web interface.
The password must satisfy the following requirements:
 - Must not be the same as the user name.
 - Must not contain dictionary words, popular combinations of letters, or examples of a keyboard layout (for example, Qwerty or passw0rd).
 - Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
 8. In the **Confirm password** field, re-enter the password that will be used to access the web interface.
 9. Click the **Add** button.

This will create an administrator account for the program web interface.

If you are using multitenancy mode, the administrator account of the PCN server web interface can access the data of all organizations associated with this server.

Creating a user account for the program web interface

You can create user accounts with the **Senior security officer** and **Security officer** roles.

► *To create a user account for the program web interface:*

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Click the **Add** button.

This opens the **New user** window.

4. To enable an account, turn on the **Status** toggle switch.

By default, the account is enabled.

If a user account is enabled, the user is allowed to access the program web interface. If a user account is disabled, the user is prohibited from accessing the program web interface.

5. In the **Role** drop-down list, select one of the following roles:
 - **Senior security officer.**
 - **Security officer**
6. In the **User name** field, enter a user name for the account you want to create.
The user name must meet the following requirements:
 - Must be unique in the list of user names (case-sensitive).

- Must contain no more than 32 characters.
 - Can contain letters A-Z, a-z, numbers 0-9, hyphens (-), and underscores (_).
 - Must begin with a letter (A-Z or a-z).
7. In the **New password** field, enter a user password that will be used to access the web interface.
- The password must satisfy the following requirements:
- Must not be the same as the user name.
 - Must not contain dictionary words, popular combinations of letters, or examples of a keyboard layout (for example, Qwerty or passw0rd).
 - Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
8. In the **Confirm password** field, re-enter the user password that will be used to access the web interface.
9. In the **Access** section, configure access rights:
- a. Turn on the **SCN web interface** switch to allow the user to access not only the web interface of this PCN server, but also to web interfaces of all available SCN servers.
 - b. To the right of the **Companies** setting name, select check boxes of one or more organizations to whose web interfaces you want to allow access.
- You can use the **Select all** and **Deselect all** links to select or cancel selection of all companies.
10. Click the **Add** button.
- The program user account will be created.

Changing access rights of a program web interface user account

You can change access rights of users with **Senior security officer** and **Security officer** roles for accessing PCN and SCN servers as well as organizations that are involved with these servers.

► *To change access rights of a program web interface user account, perform the following actions in the web interface of the PCN:*

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Select the account for which you want to change access rights.
This opens the **Edit account** window.
4. If you want to enable or disable an account, move the **Status** toggle switch.
5. In the **Access** section, move the **SCN web interface** toggle switch as necessary:

- Set the toggle switch to **Enabled** if you want to grant the user access to web interfaces of all available SCN servers in addition to the web interface of this PCN server.
 - Set the toggle switch to **Disabled** if you want to grant the user access only to the web interface of this PCN server.
6. To the right of the **Companies** setting name, select or clear check boxes of one or more organizations for which you want to change web interfaces access rights.
You can use the **Select all** and **Deselect all** links to select or cancel selection of all organizations.
 7. Click the **Save** button.

The access rights of the account are changed.

Enabling and disabling an administrator account or user account of the program web interface

► *To enable or disable an administrator account or user account for the program web interface, perform the following actions in the web interface of the PCN:*

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. In the list of accounts, select the user account that you want to enable or disable.
4. In the **Status** column do one of the following:
 - Turn on the toggle switch next to the name of an account if you want to enable the account.
 - Turn off the toggle switch next to the name of an account if you want to disable the account.

The action confirmation window is displayed.

5. Click **Yes**.

The state of the account is modified.

Changing the password of a program administrator or user account

► *To change the password of a program administrator account or user account, perform the following actions in the web interface of the PCN:*

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. In the list of accounts, select the account whose password you want to change.

This opens the **Edit account** window.

4. In the **New password** field, enter a new password for the program web interface.

The password must satisfy the following requirements:

- Must not be the same as the user name.

- Must not contain dictionary words, popular combinations of letters, or examples of a keyboard layout (for example, Qwerty or passw0rd).
 - Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
5. In the **Confirm password** field, enter the new password again.
 6. Click the **Save** button.

The password of the program administrator account or user account will be changed.

Changing the password of your account

► *To change the password of your account:*

1. Sign in to the web interface with your account.
 2. In the lower part of the program web interface window, click the link with the name of your account to expand the action list.
 3. Select the **Change password** action.
- This opens the **Change password** window.
4. In the **Old password** field, enter the current password for the program web interface.
 5. In the **New password** field, enter a new password for the program web interface.

The password must satisfy the following requirements:

- Must not be the same as the user name.
 - Must not contain dictionary words, popular combinations of letters, or examples of a keyboard layout (for example, Qwerty or passw0rd).
 - Must contain at least 8 characters.
 - Must contain at least three types of characters:
 - Uppercase character (A-Z).
 - Lowercase character (a-z).
 - Number.
 - Special character.
6. In the **Confirm password** field, enter the new password again.
 7. Click the **Change password** button.

This will change your user account password for accessing the program web interface.

Participation in Kaspersky Security Network and use of Kaspersky Private Security Network

To protect the user's computer more effectively, Kaspersky Anti Targeted Attack Platform uses data that is collected from users around the globe. *Kaspersky Security Network* is designed to collect such data.

Kaspersky Security Network (hereinafter also "KSN") is an infrastructure of online services that provides users with access to the Kaspersky Lab online knowledge base containing information on the reputation of files, web resources, and software. Use of data from Kaspersky Security Network ensures that Kaspersky Anti Targeted Attack Platform responds faster to new objects that have not yet been added to the anti-virus databases, improves the performance of some protection components, and reduces the likelihood of false alarms.

Thanks to users who participate in Kaspersky Security Network, Kaspersky Lab is able to promptly receive information about the types and sources of objects that have not yet been added to the anti-virus databases, develop solutions for neutralizing them, and minimize the number of false alarms. User participation also helps other users of Kaspersky Security Network promptly receive information about threats to the IT infrastructure of their organizations.

When you participate in Kaspersky Security Network, Kaspersky Anti Targeted Attack Platform sends Kaspersky Security Network requests about the reputation of files, web resources and software, and receives a response containing data about the reputation of those objects.

Participation in Kaspersky Security Network is voluntary. The decision to participate in Kaspersky Security Network is made during installation of Kaspersky Anti Targeted Attack Platform, and that decision can be changed at any time.

For more details about participation in Kaspersky Security Network, please read the [Kaspersky Security Network Statement](#).

If you do not want to participate in KSN, you can use Kaspersky Private Security Network (hereinafter also referred to as "KPSN"). KPSN is a solution that allows users to access the reputation databases of Kaspersky Security Network and other statistical data without actually sending data from their own computers to Kaspersky Security Network.

If you want to purchase Kaspersky Private Security Network, you can contact Kaspersky Lab partners in your region.

Participation in KSN is configured on the Central Node server and is applied to all connected Sensor servers. If you are using distributed solution and multitenancy mode, configure participation in KSN on the PCN server. Configured participation in KSN is applied to all SCN servers connected to the PCN.

Viewing the KSN Statement and configuring participation in KSN

► *To configure participation in Kaspersky Security Network:*

1. Log in to the program web interface with the administrator account.
2. Select the **Settings** section, **Participation in KSN/KPSN** subsection.
3. On the right of the **Connection type** parameter name, click the **KSN** button.
4. Carefully read the Kaspersky Security Network Statement and select one of the following options:
 - **I agree to participate in KSN**, if you accept the terms of the KSN Statement and want to participate in KSN.
 - **I do not agree to participate in KSN**, if you do not accept the terms of the KSN Statement and do not want to participate in KSN.

If you do not agree with the terms of the Statement, use of Kaspersky Security Network will not be enabled.

5. Click the **Apply** button.

Participation in Kaspersky Security Network will be configured.

Enabling the use of KPSN

► *To enable the use of KPSN:*

1. Log in to the program web interface with the administrator account.
2. Select the **Settings** section, **Participation in KSN/KPSN** subsection.
3. On the right of the **Connection type** parameter name, click the **KPSN** button.
4. In the **KPSN configuration files** section, upload the `kc_private.xml`, `kh_private.xml` and `ksncli_private.dat` files by using the **Browse** button.
5. Click the **Apply** button.

Use of Kaspersky Private Security Network will be enabled.

Configuring a connection to a local reputation database of KPSN

The program can save information about Sandbox component alerts to the local reputation database of KPSN. In this case, the *Untrusted* status is assigned to objects. Data of local reputation databases is available only to corporate LAN computers.

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To configure the connection of Kaspersky Anti Targeted Attack Platform to a local reputation database of KPSN:*

1. Log in to the program web interface with the administrator account.

2. Select the **Settings** section, **KPSN reputation database** subsection.
3. In the **Host** field, specify the IP address of the KPSN server on which the local reputation database of KPSN is stored.
4. Click the **Browse** button to the right of the **TLS certificate** field.
The file selection window opens.
5. Select the certificate file for user authentication in KPSN and click the **Open** button.
6. Click the **Browse** button to the right of the **TLS encryption key** field.
The file selection window opens.
7. Select the file containing the private encryption key, and click the **Open** button.

The connection to the local reputation database of KPSN will be configured.

Configuring information to be saved to a local reputation database of KPSN

The program can save information about Sandbox component alerts to the local reputation database of KPSN. In this case, the *Untrusted* status is assigned to objects. Data of local reputation databases is available only to corporate LAN computers.

► *To configure the saving of information about alerts to the local reputation database of KPSN:*

1. Log in to the program web interface under the senior security officer account.
2. Select the **Settings** section, **KPSN rules** subsection.
3. In the **Alert importance** settings group, select the check boxes depending on the importance level of alerts whose information you want to save in the local reputation database of KPSN.
4. Click the **Save** button.

Information about alerts of the selected importance level will be saved in the local reputation database of KPSN.

Declining participation in KSN and use of KPSN

► *To decline participation in Kaspersky Security Network and the use of KPSN:*

1. Log in to the program web interface with the administrator account.
2. Select the **Settings** section, **Participation in KSN/KPSN** subsection.
3. On the right of the **Connection type** parameter name, click the **Not connected** button.
4. Click the **Apply** button.

You will not participate in KSN and will not use KPSN.

Managing the Sandbox component through the web interface

The Sandbox web interface is located on the server hosting the Sandbox component.

The Sandbox web interface is protected against *CSRF attacks* and operates only if the web interface user's browser provides the Referrer header of an HTTP POST request. Make sure that the browser that you are using to work with the Sandbox web interface does not modify the Referrer header of an HTTP POST request. If the connection with the web interface is established through a proxy server of your organization, check the settings and make sure that the proxy server does not modify the Referrer header for an HTTP POST request.

► *To begin working with the Sandbox web interface, proceed as follows:*

1. In a browser on any computer on which access to the server with the Sandbox component is allowed, enter the IP address of the server with the Sandbox component (see page [103](#)).

The Sandbox component administrator credentials input window opens.

2. Enter the Sandbox component administrator user name and password that you specified when installing the Sandbox component (see page [102](#)).

You can now start working in the Sandbox web interface.

If you use more than one servers with the Sandbox component, configure settings of each Sandbox component from the Sandbox web interface of such server.

Updating the Sandbox component databases

The Sandbox component databases are files with records that make it possible to detect a malicious code and signs of suspicious behavior in scanned objects.

Virus analysts at Kaspersky Lab detect hundreds of new threats daily, create records to identify them, and include them in *database updates packages* (or update packages). Update packages consist of one or more files containing records to identify threats that were detected since the previous update package was released. We recommend that you regularly receive update packages.

During the license validity period, you can obtain update packages automatically once every hour or update the databases manually.

Updating databases manually

► *To start a database update manually:*

1. Select the **Database Update** section in the Sandbox web interface window.

The **Last update** settings group will show time and status of the last Sandbox database update.

2. Click the **Start** button.

Selecting a database update source

► *To select a database update source, proceed as follows:*

1. Select the **Database Update** section in the Sandbox web interface window.
2. In the **Update source** settings group, select a source from which you want to receive update packages:
 - **Kaspersky Lab update server.**
 - **Custom server.**
3. If you selected **Custom server**, in the field under the name of this parameter, enter the URL address of the update package on your FTP or HTTP server or the full path to the folder with the update package.
4. Click **Apply** in the lower part of the window.

Enabling and disabling a proxy server for database update

► *To enable or disable a proxy server for the Sandbox component database update, proceed as follows:*

1. Select the **Database Update** section in the Sandbox web interface window.
2. In the workspace, do one of the following:
 - Enable the switch next to the **Proxy server** settings group name if you want to use the proxy server for the Sandbox component database update.
 - Disable the switch next to the **Proxy server** settings group name if you do not want to use the proxy server for the Sandbox component database update.

Configuring proxy server connection settings for database update

► *To configure proxy server connection settings for the Sandbox component database update, proceed as follows:*

1. Select the **Database Update** section in the Sandbox web interface window.
2. Enable the switch next to the **Proxy server** settings group name.
3. In the **Address** field, enter the proxy server address.
4. In the **Port** field, enter the proxy server port number.
5. In the **User name** field, enter the proxy server user name.
6. In the **Password** field, enter the password to obtain connection to the proxy server.
7. Do one of the following:
 - Select the check box **Bypass proxy server for local addresses**, if you do not want to use the proxy server for internal emails of your organization.
 - Clear the **Bypass proxy server for local addresses** check box if you want to use the proxy server irrespective of email affiliations to your organization.
8. Click **Apply** in the lower part of the window.

Configuring connection between the Sandbox and Central Node components

The following procedure is used to configure the Sandbox component connection with the Central Node component:

1. In the administrator menu or in the web interface of each server hosting the Central Node component, a request for connection to the Sandbox component is created.
2. The Sandbox web interface shows connection requests.

You can accept or reject each request.

Creating a request for connection to Sandbox in the Central Node administrator menu

To create a connection between the Central Node and Sandbox components, you should send a request for connection to the Sandbox component from each Central Node component.

► *To create a request for connection to the Sandbox component, proceed as follows:*

1. Log in to the console of the Central Node server, from which you want to create a request for connection to Sandbox, via the SSH protocol or through a terminal.
2. In response to the system prompt, enter the admin user name and password set during installation and configuration of the Central Node component.

The program administrator menu is displayed.

3. In the program administrator menu, select **Program Settings**.
4. Press **ENTER**.

The action selection window opens.

5. Select **Configure Sandbox Connection**.
6. Press **ENTER**.

This opens the **Sandbox Access** window.

7. Select **New**.
8. Press **ENTER**.

This opens the **Sandbox Node** window.

9. In the **Sandbox Name** field, enter the domain name of the Sandbox server, the request for connection to which you are creating.
10. In the **Sandbox Node** field, enter IP address of the Sandbox server, the request for connection to which you are creating.
11. Click **Ok**.

The action selection window opens.

12. Select the line containing the Sandbox server IP address.
13. Press **ENTER**.

14. This opens the **Sandbox Key Fingerprint** window containing the Sandbox certificate thumbprint and a request to confirm the certificate thumbprint authenticity.
15. Make sure that this certificate thumbprint matches that in the web interface of the Sandbox server, the request for connection to which you are creating.
16. After making sure that the certificate thumbprints are identical, click **Yes**.

This opens a window prompting you to confirm sending the request for connection to the Sandbox component.

17. Click **Yes**.

You will return to the action selection window with the Sandbox server IP address.

If the request for connection to the Sandbox component is sent successfully, the value **Yes** will be displayed opposite the Enabled parameter name.

Processing connection requests from the Central Node servers in the Sandbox web interface

You can accept, reject or revoke a previously accepted connection request from the Central Node servers in the Sandbox web interface.

► *To accept, reject or revoke a connection request from the Central Node servers, proceed as follows:*

1. Select the **KATA Authorization** section in the window of the Sandbox web interface.

The **Central Node connection requests** section will show a list of connection requests from the Central Node components.

Each connection request contains the following information:

- **IP**—IP address of the Central Node server.
- **Certificate fingerprint**—Thumbprint of the Central Node TLS certificate used to establish an encrypted connection between servers.
- **State**—Status of the connection request.

May have the values **Pending** or **Accepted**.

2. Make sure that the Central Node certificate thumbprint matches the certificate thumbprint configured for the Central Node.

You can check the Central Node certificate thumbprint from the Central Node server administrator menu in the **Manage Server Certificate** section.



3. Click one of the following buttons in the line containing the connection request from the Central Node component:
 - **Accept** if you want to accept the connection request.
 - **Reject** if you want to reject the connection request.
 - **Revoke** if you want to revoke a previously accepted connection request.
4. Click **Apply** in the lower part of the window.

Configuring the Sandbox component network interfaces

This section describes configuration of the Sandbox component network interfaces.

Configuring DNS settings

► *To configure DNS settings:*

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Host name** field, enter the name of the server on which you are installing the Sandbox component in FQDN format (for example, sandbox).
3. To the right of the **DNS servers** parameter name, click the **Add** button.
This will add an empty field for the DNS server IP address input.
4. Enter the IP address of the primary DNS server in IPv4 format.
5. Click the  button to the right of the entry field.
The DNS server will be added.
6. If you want to add an additional DNS server, repeat steps 2-5.
7. If you want to remove a previously added DNS server, click the  button to the right of the line containing the DNS server IP address.

You can only remove additional DNS servers. You cannot remove the primary DNS server. If you added 2 and more DNS servers, you can remove any of them, and the remaining DNS server will be used as the primary server.

Configuring settings of the management network interface

A management network interface is intended for providing access to the server with the Sandbox component via the SSH protocol, and the Sandbox component will also receive objects from the Central Node component via this interface.

You can configure a management network interface during installation of the Sandbox component (see page [102](#)).

You can also configure a management network interface from the Sandbox web interface.

► *To configure a management network interface from the Sandbox web interface, proceed as follows:*

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Management interface** settings group from the **Interface** drop-down list, select a network interface, which you want to use as a management interface.
3. In the **IP** field, enter the IP address that you want to assign to this network interface if no IP address is assigned.
4. In the **Mask** field, enter the network mask in which you want to use this network interface.
5. Click **Apply** in the lower part of the window.

Configuring settings of a network interface used for Internet access of processed objects

Objects processed by the Sandbox component may attempt activities on the Internet via the network interface used for Internet access of processed objects. The Sandbox component can analyze the behavior of these objects.

If you block Internet access, the Sandbox component cannot analyze the behavior of objects on the Internet, and will therefore only analyze the behavior of objects without Internet access.

The network interface used for Internet access of processed objects must be isolated from the local network of your organization.

If the security policy of your organization denies access to the Internet from computers of local network users, and you have configured the Sandbox network interface for Internet access of processed objects, there is a risk of the following scenario:

A hacker can attach a malicious program to a random file and initiate a Sandbox scan of this file from the computer of a local network user. This file will be taken over outside the local network through the network interface used for Internet access of processed objects in the course of scanning the file by the Sandbox component.

Unavailability of the Sandbox network interface for Internet access of processed objects eliminates any risk of such data transfer but compromises the quality of alerts.

► To configure a network interface used for Internet access of processed objects, proceed as follows:

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Internet interface** settings group from the **Interface** list, select a network interface that you want to use for Internet access of processed objects.

The management network interface that you configured previously cannot be selected from this list of network interfaces.


3. In the **IP** field, enter the IP address that you want to assign to this network interface.
4. In the **Mask** field, enter the network mask in which you want to use this network interface.
5. In the **Default gateway** field, enter the gateway address of the network in which you want to use this network interface.
6. Click **Apply** in the lower part of the window.

Adding, changing and removing static network routes


You can configure static network routes during installation of the Sandbox component (see page [103](#)).

You can also add, remove or change static network routes from the Sandbox web interface.



► *To add a static network route, proceed as follows:*

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Static Routes** settings group, click the **Add** button.
A line with empty fields will be added in the list of static network routes.
3. In the **IP** field, enter the IP address of the server for which you want to configure a static network route.
4. In the **Mask** field, enter the subnet mask.
5. In the **Gateway** field, enter the IP address of the gateway.
6. From the **Interface** list, select a network interface for which you want to add a static network route.
7. Click .
8. Click **Apply** in the lower part of the window.

► *To remove a static network route, proceed as follows:*

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Static Routes** settings group in the line containing the static network route that you want to remove, click the  button.
3. Click **Apply** in the lower part of the window.

► *To change a static network route, proceed as follows:*

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Static Routes** settings group in the line containing the static network route that you want to change, click the  button.
The static network route line will become editable. You can change one or more parameters of a static network route.
3. In the **IP** field, change the IP address of the server for which you want to configure a static network route.
4. In the **Mask** field, change the subnet mask.
5. In the **Gateway** field, change the IP address of the gateway.
6. From the **Interface** list, select the network interface for which you are editing the network route.
7. Click .
8. Click **Apply** in the lower part of the window.

Updating the Sandbox system

Kaspersky Lab can issue update packages for Kaspersky Anti Targeted Attack Platform and individual program components. For example, there can be issued urgent update packages eliminating vulnerabilities and errors, scheduled updates adding new or improving existing features of the program and its components.

After Sandbox updates have been issued, you can install them through the Sandbox web interface.

Prior to installing updates through the Sandbox web interface, you need to download an update package in TGZ format and the instructions for installing this update from the Kaspersky Lab website to your computer.

► *To update the Sandbox system through a web interface, proceed as follows:*


1. Select the **System Upgrade** section in the window of the Sandbox web interface.
To the right of the **Current program version** parameter name, the current version of the Sandbox component will be displayed.
2. Click the **Browse** button to the right of the **Upgrade package** field.
The file selection window opens.
3. Select an update file to download and click the **Open** button.
The file selection window closes.

You can keep track of the Sandbox system update progress in the **Upgrade log** window of the **System Upgrade** section of the Sandbox web interface.

The update package will be installed automatically. The update process can take a while. The Sandbox server will restart. The Sandbox component will be unavailable during the system update.

Setting the Sandbox system date and time

► *To set a date and time of the server hosting the Sandbox component, proceed as follows:*

1. In the Sandbox web interface window, select **Date and Time**.
2. In the **Country** drop-down list, select the relevant country.
3. In the **Time zone** drop-down list, select the relevant time zone.
4. If you prefer to synchronize the time with the NTP server, select **Synchronization with NTP servers**.
5. If you prefer to set the date and time manually, do not enable the switch to the right of the **Synchronization with NTP servers** parameter name and proceed as follows:
 - a. In the **Date** field, enter the current date or click the  button and select a date in the calendar.
 - b. In the **Time** field, enter the current time.
6. Click **Apply** in the lower part of the window.

Installing and configuring images of operating systems and software required for the operation of the Sandbox component

The distribution kit includes three ISO images of Windows XP SP3, 64-bit Windows 7, and 64-bit Windows 10 operating systems, as well as software required for the operation of the Sandbox component. You do not have to activate these operating systems and applications. The images already include a Microsoft license key.

The Sandbox component starts objects in these operating systems and analyzes the behavior of these objects to in order to detect malicious activity and signs of targeted attacks and intrusions into the corporate IT infrastructure.

In case of problems with activation of operating systems or software, the web interface of the Sandbox component displays an error message. If this happens, please contact Kaspersky Lab Technical Support.

Downloading ISO images of operating systems and software required for the operation of the Sandbox component

► To download an ISO image of an operating system and software required for the operation of the Sandbox component, do the following for each ISO image:

1. Select the **Virtual Machines** section in the window of the Sandbox web interface.
2. In the **Virtual Machine images** settings group, click the **Upload** button.
The file selection window opens.
3. Select an ISO file that you want to download and click the **Open** button.
The file selection window closes.

The **Virtual Machine images** list shows the downloaded image of the operating system and software required for operation of the Sandbox component.

Proceed with downloading images of operating systems and software required for the operation of the Sandbox component for each ISO image.

Creating virtual machines with images of operating systems and software required for the operation of the Sandbox component

► To create a virtual machine with an image of an operating system and software required for the operation of the Sandbox component, do the following for each virtual machine:

1. Select the **Virtual Machines** section in the window of the Sandbox web interface.
2. In the **Virtual Machine images** list, in the line containing the name of the image of the operating system and software required for the operation of the Sandbox component, click **Create VM**.

This opens the **EULA** window containing texts of the following End User License Agreements:

- MICROSOFT WINDOWS 7 PROFESSIONAL SERVICE PACK 1.
- MICROSOFT WINDOWS XP PROFESSIONAL EDITION SERVICE PACK 3.
- MICROSOFT OFFICE 2010 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2007 DESKTOP APPLICATION SOFTWARE.
- MICROSOFT OFFICE 2003 DESKTOP APPLICATION SOFTWARE.

- ADOBE® Personal Computer Software License Agreement.
 - MICROSOFT VISUAL C++ 2005 RUNTIME LIBRARIES.
 - MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64), SERVICE PACK 1.
 - MICROSOFT VISUAL C++ 2010 RUNTIME LIBRARIES.
 - MICROSOFT VISUAL C++ 2012 RUNTIME LIBRARIES.
 - MICROSOFT VISUAL C++ REDISTRIBUTABLE FOR VISUAL STUDIO 2013.
 - MICROSOFT VISUAL STUDIO 2017 TOOLS, ADD-ONS and C++ REDISTRIBUTABLE.
3. Read the End User License Agreements and click the **Accept** button in the right lower corner of the **EULA** window.
The **Unpack** window opens. The archive containing an image of the operating system and software required for the operation of the Sandbox component is unpacked.
 4. The **Not installed Virtual Machines** list of the **Virtual Machines** window shows the virtual machine, which is ready for activation of the operating systems and software as well as for installation.

Proceed with creating virtual machines with images of operating systems and software required for the operation of the Sandbox component for each virtual machine.

Installing virtual machines with images of operating systems and software required for the operation of the Sandbox component

- *To install all ready-to-install virtual machines with images of operating systems and software required for operation of the Sandbox component:*

1. Select the **Virtual Machines** section in the window of the Sandbox web interface.
2. In the left lower corner of the **Not installed Virtual Machines** list, click the **Install ready VMs** button.

Virtual machines with operating systems, next to the names of which the **Not installed Virtual Machines** list shows the **Ready to install** status, will be installed and shown in the list at the top of the **Virtual Machines** window.

Deleting all pending virtual machines

- *To delete all pending virtual machines, proceed as follows:*

1. Select the **Virtual Machines** section in the window of the Sandbox web interface.
2. In the left lower corner of the **Not installed Virtual Machines** list, click the **Delete all pending VMs** button.

Pending virtual machines with operating systems and applications required for operation of the Sandbox component are deleted.

Setting the maximum number of simultaneously running virtual machines

Set a limit on the number of simultaneously running virtual machines with operating systems in which the Sandbox component will process objects.

The number of simultaneously running virtual machines cannot exceed 200.

Calculate the number of simultaneously running virtual machines with images of operating systems as follows: multiply the number of processor cores by 1.5.

► *To set the maximum number of simultaneously running virtual machines:*

1. Select the **Virtual Machines** section in the window of the Sandbox web interface.
2. In the **Guest Virtual Machines** settings group in the **Maximum simultaneous VMs** field, enter the number of simultaneously running virtual machines.

You can enter a number ranging from 1 to 200.

3. Click the **Save** button.

Downloading the Sandbox system log to the hard drive

Log data in the Sandbox system is stored in open, non-encrypted form. The data is stored for the last 7 days.

► *To download the Sandbox system log to the hard drive, proceed as follows:*

1. Select the **Administration** section in the Sandbox web interface window.
2. In the **System Log** settings group, click the **Download** button.

The Sandbox system log is downloaded to your computer's hard drive into the folder set as the file download folder in the settings of the browser that you use for working with the program.

Exporting the Sandbox parameters

► *To export the Sandbox system parameters, proceed as follows:*

1. Select the **Administration** section in the Sandbox web interface window.
2. In the **Settings** settings group, click the **Export** button.

This opens the **Warning** window containing a warning on specifics of exporting the system parameters.

The Sandbox system parameters are dependent on hardware and software parameters of the server, on which the Sandbox component is installed. The Sandbox system exported parameters are intended to be imported to the same or another server strictly identical in configuration. Any attempt to restore the configuration of the Sandbox system with parameter values saved to another Sandbox system may disrupt the Sandbox system.

3. Click the **Save** button.

A tar.gz file is downloaded to your computer's hard drive into the folder set as the file download folder in the settings of the browser that you use for working with the program. The file contains all the Sandbox system current parameters.

Archives with backup copies of the system parameters can contain confidential information, such as passwords and privacy keys. The Kaspersky Anti Targeted Attack Platform administrator must independently ensure the security of this data.

Importing the Sandbox parameters

► *To import the Sandbox parameters, proceed as follows:*

1. Select the **Administration** section in the Sandbox web interface window.
2. In the **Settings** settings group, click the **Import** button.

This opens the **Warning** window containing a warning on specifics of importing the system parameters.

The Sandbox component parameters are dependent on hardware and software parameters of the server, on which the Sandbox is installed. The Sandbox exported parameters are intended to be imported to the same or another server strictly identical in configuration. Any attempt to restore the configuration of one Sandbox system with parameter settings saved to another Sandbox system may disrupt the system.

3. Click the **Restore** button.

The file selection window opens.

4. Select a tar.gz file with the Sandbox parameters that you want to download and click the **Open** button.

The file selection window closes.

If the Sandbox parameters have been successfully imported, the Sandbox server will restart. A few minutes later, you need to refresh the browser window and log in again.

Archives with backup copies of the system configuration can contain confidential information, such as passwords and privacy keys. The Kaspersky Anti Targeted Attack Platform administrator must independently ensure the storage security of this data.

Restarting the Sandbox server

► *To restart the Sandbox server, proceed as follows:*

1. Select the **Administration** section in the Sandbox web interface window.
2. In the **Power** settings group, click the **Restart** button.
This opens the Sandbox server restart confirmation window.
3. Click **Yes**.

The Sandbox server will restart. In a few minutes, you will be able to log in to the system.

Shutdown of the Sandbox server

► *To shut down the Sandbox server, proceed as follows:*

1. Select the **Administration** section in the Sandbox web interface window.
2. In the **Power** settings group, click the **Power off** button.
This opens the Sandbox server shutdown confirmation window.
3. Click **Yes**.

The Sandbox server will shut down.

Changing the Sandbox administrator account password

► *To change the Sandbox administrator account password, proceed as follows:*

1. Select the **Administration** section in the Sandbox web interface window.
2. The **Change password** settings group will show the Sandbox administrator account name that you set during installation of the Sandbox (see page [102](#)) and the fields for changing the password.
3. In the **Current password** field, enter the current password for the Sandbox administrator account.
4. In the **New password** field, enter a new password for the Sandbox administrator account.
5. In the **Confirm password** field, enter the new password for the Sandbox administrator account again.
6. Click the **Change password** button.

The Sandbox administrator account password will be changed.

For an administrator: Getting started with the program web interface

This section is intended for professionals who install and administer Kaspersky Anti Targeted Attack Platform and manage PCN and SCN servers and organizations in distributed solution and multitenancy mode.

Kaspersky Anti Targeted Attack Platform Interface

The program is managed through the web interface. Sections of the program web interface differ depending on the role of the user: **Administrator** or **Senior security officer / Security officer** (see page [229](#)).

The window of the program web interface contains the following items:

- Sections in the left part and in the lower part of the program web interface window.
- Tabs in the upper part of the program web interface window for certain sections of the program.
- The workspace in the lower part of the program web interface window.

Sections of the program web interface window

The program web interface for the **Administrator** role is divided into the following sections:

- **Dashboard**. Contains Kaspersky Anti Targeted Attack Platform Monitoring data.
- **Operation mode**. Contains information about PCN and SCN servers about organizations in distributed solutions and multitenancy mode.
- **Endpoint Sensors**. Contains information about connected Endpoint Sensors components and their settings.
- **Settings**. Contains the settings of the server with the Central Node component.
- **Sensor servers**. Contains information about connected Sensor components and their settings.
- **Sandbox servers**. Contains information about the connection of the Central Node component to Sandbox components.
- **External systems**. Contains information about program integration with mail sensors.

Workspace of the program web interface window

The workspace displays the information you choose to view in the sections and on the tabs of the program web interface window. It also contains control elements that you can use to configure how the information is displayed.

Monitoring program operation

You can monitor program operation using the widgets in the **Dashboard** section of the program web interface window. You can add, delete and move widgets, configure the scale of widgets, and select the data display period.

About widgets and layouts

You can use widgets to monitor program operation.

The *layout* is the appearance of the workspace of the program web interface window in the **Dashboard** section. You can add, delete, and move widgets on the layout.

The following widgets are available in the program:

- **Data processing.** Displays the status of traffic processing by the Sensor component.
- **Queues** (see page [184](#)). Displays information on the number and volume of objects waiting to be scanned by the program modules and components.
- **Sandbox processing time** (see page [185](#)). Displays the average time taken to receive the scan results after objects were scanned by the Sandbox component.

If you are using the multitenancy mode, the section displays data on the organization and server that you chose (see page [181](#)).

Selecting an organization and a server to manage in the Dashboard section

If you are using multitenancy mode, prior to using the **Dashboard** section, you need to select the organization and server whose data you want to view.



► *To select an organization and server whose data you want to display in the **Dashboard** section:*

1. In the upper part of the program web interface menu, click the arrow next to the server name.
2. In the drop-down list, select the organization and server from the list.

Data for the selected server is displayed. If you want to select a different organization and server, you need to repeat the organization and server selection procedure.

Adding a widget to the current layout


► *To add a widget to the current layout:*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.
3. In the drop-down list, select **Customize**.
4. Click the **Widgets** button.
5. In the **Manage widgets** window that opens:
 - If you want to add the **Queues** widget, switch on the toggle button next to the name of this widget.
 - If you want to add the **Sandbox processing time** widget, switch on the toggle button next to the name of this widget.
 - If you want to add the **Data processing** widget, click the  button next to the name of this widget.

The selected widget will be added to the current layout.

Moving a widget in the current layout

► *To move a widget in the current layout:*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.
3. In the drop-down list, select **Customize**.
4. Select the widget that you want to move within the layout.
5. Left-click and hold down the left mouse button on the upper part of the widget to drag the widget to another place on the layout.

6. Click the **Save** button.

The current layout will be saved.


Removing a widget from the current layout

► *To remove a widget from the current layout:*

1. Select the **Dashboard** section in the program web interface window.

2. In the upper part of the window, click the  button.

3. In the drop-down list, select **Customize**.

4. Click the  icon in the upper right corner of the widget that you want to remove from the layout.

The widget will be removed from the workspace of the program web interface window.

5. Click the **Save** button.

The widget will be removed from the current layout.

Saving a layout to PDF

► *To save a layout to PDF:*

1. Select the **Dashboard** section in the program web interface window.

2. In the upper part of the window, click the  button.

3. In the drop-down list, select **Save as PDF**.

This opens the **Saving as PDF** window.

4. In the lower part of the window, in the **Layout** drop-down list, select the page orientation.

5. Click the **Download** button.

The layout in PDF format will be saved to the hard drive of your computer in the downloads folder of the browser.

6. Click the **Close** button.

Configuring the period for displaying data in widgets

You can configure the display of data on widgets for the following periods:

- **Day**
- **Week**
- **Month**

► *To configure the display of data on widgets for a 24-hour period (from 00:00 to 23:59):*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper-right corner of the program web interface window, in the drop-down list of data display periods, select **Day**.
3. In the calendar to the right of the **Day** period name, select the date for which you want to obtain data on the widget.

All widgets on the **Dashboard** page display data for the period you selected.

► *To configure the display of data on widgets for a week (Monday through Sunday):*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper-right corner of the program web interface window, in the drop-down list of data display periods, select **Week**.
3. In the calendar to the right of the **Week** period name, select the week for which you want to obtain data on the widget.

All widgets on the **Dashboard** page display data for the period you selected.

► *To configure the display of monthly data (calendar month) on widgets:*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper-right corner of the program web interface window, in the drop-down list of data display periods, select **Month**.
3. In the calendar to the right of the **Month** period name, select the month for which you want to obtain data on the widget.

All widgets on the **Dashboard** page display data for the period you selected.

Monitoring the receipt and processing of incoming data

On the **Data processing** widget, you can assess the processing status of data coming from the Sensor component to the server with the Central Node component, and track data drops.

You can select the Sensor whose transmitted data you want to assess in the drop-down list to the right of the **Data processing** widget name.

You can select the type of data display in the drop-down list to the right of the Sensor list:

- **Current load**—The last 5 minutes.
- **Selected period**. In this case, you can also configure the period of data display on widgets (see page [182](#)).

The left part of each widget displays the key of colors used on the specific widget.

If the **Current load** data display type is selected, the average data processing rate over the past 5 minutes is displayed to the right of the key.

Example:

The **Data processing** widget, on which the (**SPAN**) Sensor type and the **Current load** data display type are selected, displays the rate of processing data of mirrored local network traffic coming from the Sensor

component to the server with the Central Node component over a specific time period.

The following data is displayed:

- **Traffic**—Rate of incoming traffic to the server with the Sensor component, indicated in green.
- **Files**—Rate of file processing indicated in gray.
- **URLs**—Rate of URL processing indicated in blue.
- **Drops** – data processing errors indicated by vertical red lines.

When you move the mouse cursor over a widget, you will see a pop-up window that displays the data processing rate for a specific time period.

If the **Selected period** data display type is selected, to the right of the key you will see the average rate of incoming traffic to the server with the Central Node component and the number of objects processed during the selected period.

Example:

The **Data processing** widget, on which the **(SMTP)** Sensor type and the **Selected period** data display type are selected with the data display period(see page [182](#)) configured for a **Month**, displays the rate of incoming mail traffic over the SMTP protocol to the server with the Central Node component, as well as the number of files and URL addresses extracted from mail traffic for the selected month.

The following data is displayed:

- **Average traffic**—Rate of incoming traffic to the server with the Central Node component, indicated in green.
- **Files**—Number of extracted files indicated in gray.
- **URLs**—Number of extracted URLs indicated in blue.
- **Drops** – data processing errors indicated by vertical red lines.

When you move the mouse cursor over a widget, you will see a pop-up window that displays the rate of incoming traffic to the server with the Central Node component and the number of objects processed during a specific time period.

Monitoring the queues for data processing by program modules and components

You can use the **Queues** widget to assess the status of data processing by the **YARA** and **AM Engine** program modules and the **Sandbox** component and trace data drops.

You can select the type of data display in the drop-down list to the right of the **Queues** widget name:

- **Current load**—The last 5 minutes.
- **Selected period**. In this case, you can also configure the period of data display on widgets.

The left part of a widget displays the key of colors used on the widget.

The **Queues** widget displays the following data:

- **Number of messages** and **Data volume** processed by program modules and components:
 - **YARA**—blue.
 - **Sandbox**—violet.
 - **AM Engine** – green.
- **Drops** – data processing errors indicated by vertical red lines.

When you hover the mouse cursor over a widget, you will see a pop-up window that displays the status of data processing by the **YARA** and **AM Engine** program modules and the **Sandbox** component, as well as the data drops during a specific time period.

Monitoring the processing of data by the Sandbox component

The **Sandbox processing time** widget displays the average time that elapses from the moment data is sent to one or several servers with the Sandbox component (including the queue time prior to sending) until the results from data processing by the Sandbox component are displayed in the web interface of Kaspersky Anti Targeted Attack Platform during the selected period.

Example:

If the period of data display on widgets is configured for a **Month**, the **Sandbox processing time** widget displays orange-colored columns for each day of the month.

When you move the mouse cursor over each column, you will see a pop-up window that displays the average time that elapses from the moment data is sent to one or several servers with the Sandbox component until the results from data processing by the Sandbox component are displayed in the web interface of Kaspersky Anti Targeted Attack Platform during the selected day.

You can increase the rate at which data is processed by the Sandbox component and the throughput of the Sandbox component by increasing the number of servers with the Sandbox component and by distributing the data to be processed among those servers.

Viewing information about failures of program modules and components

In case errors are encountered in the course of operation of program modules and components, a red frame listing encountered errors is displayed in the upper part of the **Dashboard** section of the program web interface.

Users with the **Local administrator** or **Administrator** roles can access information about program failures on the Central Node, PCN, or SCN server that the user is currently managing.



Users with the **Senior security officer** or **Security officer** roles can access the following information about program failures:

- If you are using a standalone Central Node server, the user can access information about program failures on the Central Node server which the user is currently managing.
- If you are using the distributed solution and multitenancy mode, and the user is managing an SCN server, the user can access program failure information on that SCN server for organizations whose data the user is allowed to access (see page [160](#)).
- If you are using the distributed solution and multitenancy mode, and the user is managing the PCN server, the user can access program failure information on the PCN server and all SCN servers connected to that server, for organizations whose data the user is allowed to access (see page [160](#)).

► *For details about encountered failures,*

click **View details** to open the **System errors** window.

The **System errors** window displays the following information:

- If there are no operating errors, the  icon is displayed in the line.
- If problems with program operation are detected, the line displays an icon showing the quantity of errors found (for example, .


In this case, detailed error information is displayed in the right part of the **System errors** window.

The **System errors** window contains the following sections:

- **Components health**—Performance status of program modules and components.

Contains information about the operating status of the following program modules and components:

- **YARA.**
- **Sandbox.**
- **URL Reputation.**
- **Intrusion Detection System.**
- **Anti-Malware Engine.**
- **Targeted Attack Analyzer.**
- **IOC Scanner.**
- **IOA Analysis.**
- **Database update**—For all servers on which the program is running.

If the databases of one or more program components have not been updated in 24 hours, the  icon is displayed next to the name of the server on which the program modules and components are installed.

- **Quarantine.**
- **Data processing**—Presence of errors when receiving and processing incoming data. The status is generated based on the following criteria:
 - Existence of errors associated with receiving data from servers with the Sensor component and from the server or virtual machine with the mail sensor.
 - Information about exceeding the maximum allowed time that objects wait in the queue to be scanned by program modules and components.
- **Server connection**—State of the connection between the PCN server and connected SCN servers (displayed if you are using the distributed solution and multitenancy mode).

If there are problems detected in the performance of program modules or components and you cannot resolve those problems on your own, you are advised to contact Kaspersky Lab Technical Support (see page 395).

Managing Central Node, PCN, or SCN servers using the program web interface

You can use the program web interface to perform the following actions with the server on which the Central Node component is installed:

- Configure the date and time on the server.
- Power off and restart the server.
- Replace the server certificate.
- Configure the network settings of the server.

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.


Configuring the date and time on the server




If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure the date and time on the server:

1. In the window of the program web interface, select the **Settings** section, **Date and time** subsection.
2. In the **Country** drop-down list, select the country (physical location) of the server that has the Central Node component installed.
3. In the **Time zone** drop-down list, select the time zone of the physical location of the server with the Central Node component installed.

You can specify the country and time zone by selecting the relevant region on the map under the drop-down lists.

4. Configure synchronization with NTP servers:
 - Turn on the toggle switch next to the name of the **Synchronization with NTP servers** parameter if you want to enable synchronization.
 - Turn off the toggle switch next to the name of the **Synchronization with NTP servers** parameter if you want to disable synchronization.
5. In the **NTP servers** section:
 - If you want to add a new NTP server:
 - a. Click the **Add** button.
 - b. In the field that opens, enter the IP address or domain name of the NTP server.
 - c. Click the  button to the right of the field.

- If you want to edit the IP address or domain name of the NTP server, click the  button in the line containing the server.
 - If you want to delete an NTP server, click the  button in the line containing the server.
6. If synchronization with NTP servers is disabled, manually specify the date and time of the server:
- In the **Date** field, specify the current date manually or select it in the calendar by clicking the  button to the right of the field.
 - In the **Time** field, specify the current time.
7. Click the **Apply** button.
- The date and time of the server will be configured.

Powering off and restarting the server

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To power off or restart the server through the program web interface:*

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
 2. In the **Server management** settings group:
 - If you want to power off the server on which the Central Node component, PCN, or SCN is installed, click the **Power off** button.
 - If you want to restart the server on which the Central Node component, PCN, or SCN is installed, click the **Restart** button.
 3. In the confirmation window, click **Yes**.
- The server will be powered off or restarted.

Replacing the server certificate

After creating a new certificate, you must reauthorize the mail sensors, connect Central Node, PCN, or SCN to Sandbox, upload the new certificate to Active Directory, and restart the Endpoint Sensors components service.

You can create a new certificate through the program web interface or upload a previously created certificate.

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To create a new server certificate:*

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Certificate fingerprint** settings group, click the **Generate new** button.
3. In the confirmation window, click **Yes**.

The new certificate of the server will be created. Communication with the mail sensors and the Sandbox component will be interrupted until reauthorization.

Use the web interface of the PCN or SCN server to which you want to upload the certificate.

► *To upload a previously created certificate:*

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Certificate fingerprint** settings group, click the **Upload** button.
3. In the confirmation window, click **Yes**.

The certificate will be uploaded. Communication with the mail sensors and the Sandbox component will be interrupted until reauthorization.

Saving a server certificate file on a computer

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To save the server certificate file on the computer:*

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Certificate fingerprint** settings group, click the **Download** button.

The server certificate file will be saved in the downloads folder of the browser.

Assigning a server DNS name

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To assign the server name to be used by DNS servers:*

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. Enter the full domain name of the server into the **Server name (FQDN)** field.

Specify the server name in FQDN format (for example: `host.domain.com` or `host.domain.subdomain.com`).

3. Click the **Apply** button.

The host name will be assigned.

Configuring DNS settings

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure DNS settings:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. If you want to configure the assignment of DNS addresses using a DHCP server:
 - a. In the **DNS settings** settings group, in the **Mode** line, select **DHCP**.
 - b. In the **Network interface** drop-down list, select the name of the network interface used for connecting to the DNS server.
3. If you want to configure the assignment of static DNS addresses:
 - a. In the **DNS settings** settings group, in the **Mode** line, select **Static**.
 - b. In the **Domains** field, specify the domain name.
 - c. In the **Primary and Secondary DNS servers** field, enter the IP addresses of DNS servers.
4. Click the **Apply** button.

The DNS settings will be configured.

Enabling and disabling the network interface

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To enable a network interface:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. Select the network interface that you want to enable.
This opens the **Edit network interface** window.
3. In the **State** line, set the toggle switch to **Enabled**.
4. Click the **Initialize** button.

The network interface will be enabled.

► To disable a network interface:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.

2. Select the network interface that you want to disable.

This opens the **Edit network interface** window.

3. In the **State** line, set the toggle switch to **Disabled**.
4. Click the **Save** button.

The network interface will be disabled.

Configuring settings of the network interface

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure the settings of the network interface:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. Select the network interface whose settings you want to configure.
This opens the **Edit network interface** window.
3. In the **Mode** line, select one of the following options:
 - If you want the IP address of the network interface to be assigned using a DHCP server, select **DHCP**.
 - If you want to assign a static IP address to the network interface, select **Static**.
4. If you selected **Static**:
 - a. In the **IP** field, specify the IP address of the network interface.
 - b. In the **Subnet mask** field, specify the subnet mask of the network interface.
5. If you want to enable a network interface, in the **State** line, set the toggle switch to **Enabled**.
6. Click the **Initialize** button.

The settings of the network interface will be configured.

Configuring the default network route

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure the default network route:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. In the **Network route** settings group, in the **Network interface** drop-down list, select the network interface for which you want to configure the network route.
3. In the **Mode** line, select one of the following options:

- If you want to configure a network route using a DHCP server, select **DHCP**.
 - If you want to configure a static network route, select **Static**.
4. If you selected **Static**, enter the IP address of the gateway in the **Gateway** field.
 5. Click the **Apply** button.

The default network route will be configured.

Configuring proxy server connection settings

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure the proxy server connection settings:

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Proxy server** settings group, set the toggle switch to **Enabled**.
3. In the **Host** field, specify the URL of the proxy server.
4. In the **Port** field, specify the port for connecting to the proxy server.
5. In the **User name** field, specify the user name for authentication on the proxy server.
6. In the **Password** field, specify the password for authentication on the proxy server.
7. If you do not want to use a proxy server when connecting to local addresses, select the **Bypass proxy server for local addresses** check box.
8. Click the **Apply** button.

The proxy server connection settings will be configured.

Managing the Sensor component

The Sensor component receives data from network traffic and mail traffic.

You can install the Sensor and Central Node components on the same server or on separate servers. If the Sensor component is installed on a different server, you must connect it to the server with the Central Node component.

If you are using the distributed solution and multitenancy (see page [43](#)) mode, perform the necessary actions to connect to PCN or SCN servers.

Processing a connection request from the Sensor component

If you are using the distributed solution and multitenancy (see page [43](#)) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

You can accept, decline, or revoke a previously accepted connection request from the Sensor component.

► *To process a connection request from the Sensor component:*

1. Select the **Sensor servers** section in the window of the program web interface.
The **Server list** table displays the already connected Sensor components, and connection requests.
2. In the line containing the connection request of the Sensor component, perform one of the following actions:
 - If you want to connect the Sensor component, click the **Accept** button.
 - If you do not want to connect the Sensor component, click the **Reject** button.
3. In the confirmation window, click **Yes**.

The connection request from the Sensor component will be processed.

Viewing the table of servers with the Sensor component

If you are using the distributed solution and multitenancy (see page [43](#)) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

The table of servers with the Sensor component is located in the **Sensor servers** section of the program web interface window. The table contains the following information:

- **IP/name**—IP address or domain name of the server with the Sensor component.
- **Type**—Type of Sensor component. Possible values:
 - **Central Node**—The Sensor component is installed on the same server as the Central Node component.

- **Remote**—The Sensor component is installed on a different server or a mail sensor is used as the Sensor component.
- **Certificate fingerprint**—Fingerprint of the TLS certificate used to establish an encrypted connection between servers with the Sensor and Central Node components.
- **KSN/KPSN**—Status of the connection to the KSN/KPSN reputation databases.
- **SPAN**—Status of SPAN traffic processing.
- **SMTP**—Status of integration with a mail server via SMTP.
- **ICAP**—Status of integration with a proxy server via ICAP.
- **POP3**—Status of integration with a mail server via POP3.
- **State**—Status of the connection request.

Configuring the maximum size of a scanned file

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure the maximum size of a scanned file:

1. Select the **Sensor servers** section in the window of the program web interface.
The **Server list** table will be displayed.
2. Select the Sensor component for which you want to configure the maximum size of a scanned file.
A page with the Sensor component settings opens.
3. Select the **General settings** section.
4. If you want the program to scan files of any size, select the **Unlimited** check box.
5. If you want to set a maximum size for files that the program will scan:
 - a. Clear the **Unlimited** check box.
 - b. In the field under the check box, enter the maximum allowed size of a file.
 - c. In the drop-down list to the right of the field, select the unit of measurement.
6. Click the **Apply** button.

The maximum size of a scanned file will be configured.

Configuring receipt of mirrored traffic from SPAN ports

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To configure receipt of mirrored traffic from SPAN ports:*

1. Select the **Sensor servers** section in the window of the program web interface.
The **Server list** table will be displayed.
 2. Select the Sensor component for which you want to configure the receipt of mirrored traffic from SPAN ports.
A page with the Sensor component settings opens.
 3. Select the **SPAN traffic processing** section.
The **Network interfaces** table is displayed.
 4. In the line of the network interface from which you want to configure the receipt of mirrored traffic, set the toggle switch in the **SPAN traffic scanning** column to **Enabled**.
 5. In the **Capture thread** drop-down list, select the stream that will process this network interface.
 6. In the **CPU selection** drop-down list, select the processor that will process the network traffic.
 7. Click the **Apply** button.
- The receipt of mirrored traffic from SPAN ports will be configured.

Configuring integration with a mail server via SMTP

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To configure integration with a mail server via SMTP:*

1. Select the **Sensor servers** section in the window of the program web interface.
The **Server list** table will be displayed.
2. Select the Sensor component for which you want to configure integration with the mail server via SMTP.
A page with the Sensor component settings opens.
3. Select the **SMTP integration** section.
4. In the **State** field, set the toggle switch to **Enabled**.
5. In the **Destination domains** field, specify the name of the mail domain or subdomain. The program will scan email messages sent to mailboxes of the specified domains.
To disable a domain or subdomain, enclose it in the `!domain.tld` form.
If you leave the mail domain name blank, the program will receive messages sent to any email address.
6. In the **Clients** field, specify the IP addresses of hosts and/or masks of subnets (in CIDR notation) with which the program is allowed to interact over the SMTP protocol.
To disable a host or subnet, enclose the address in the `!host` form.
If you leave this field blank, the program will receive the following messages:
 - From any email addresses if you specified email domains in the **Destination domains** field.

- From a mail server in the same subnet as the server with the Sensor component if no domain is indicated in the **Destination domains** field.
7. If you want the program to receive messages of any size, in the **Message size limit** settings group, select the **Unlimited** check box.
 8. If you want to set a maximum allowed size of incoming messages:
 - a. Clear the **Unlimited** check box.
 - b. In the field under the check box, enter the maximum allowed size of a message.
 - c. In the drop-down list to the right of the field, select the unit of measurement.
 9. Click the **Apply** button.

Integration with a mail server via SMTP will be configured. The program will scan email messages received over the SMTP protocol according to the defined settings.

Configuring TLS encryption of connections with a mail server via SMTP

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► To configure TLS encryption of connections with a mail server via SMTP:

1. Select the **Sensor servers** section in the window of the program web interface.
The **Server list** table will be displayed.
2. Select the Sensor component for which you want to configure TLS encryption of connections with the mail server over the SMTP protocol.
A page with the Sensor component settings opens.
3. Select the **SMTP integration** section.
4. In the **State** field, set the toggle switch to **Enabled** if it is disabled.
5. In the **Client TLS security level** section, select one of the following options:
 - **No TLS encryption.**
The program will not employ TLS encryption of connections with a mail server.
 - **Attempt TLS encryption for incoming messages.**
The program will support TLS encryption of the connection, but encryption will not be mandatory.
 - **Require TLS encryption for incoming messages.**
The program will receive messages only over encrypted channels.
6. Click the **Download TLS Certificate** button to save the TLS certificate of the server with the Sensor component on the computer in the browser's downloads folder.
This certificate is required for authentication on the mail server.
7. In the **Requesting Client TLS certificate** section, select one of the following options:
 - **Do not request.**

The program will not verify the TLS certificate of the mail server.

- **Request.**

The program will request a TLS certificate from the mail server, if one is available.

- **Require.**

The program will receive messages only from those mail servers that have a TLS certificate.

8. Import the TLS certificate of the mail server that will be used for authentication when establishing a connection with the Sensor component. To do so:

- a. Click the **Upload TLS Certificate** button.

The file selection window opens.

- b. Select the certificate file with the PEM extension and click the Open button.

9. Click the **Apply** button.

TLS encryption of connections with the mail server over the SMTP protocol will be configured.

Enabling integration with a proxy server via ICAP

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To enable integration with a proxy server over the ICAP protocol:*

1. Select the **Sensor servers** section in the window of the program web interface.

The **Server list** table will be displayed.

2. Select the Sensor component for which you want to configure integration with a proxy server over the ICAP protocol.

A page with the Sensor component settings opens.

3. Select the **ICAP integration with proxy server** section.

4. In the **State** field, set the toggle switch to **Enabled**.

The **Host** field displays the URL of the Response Modification (RESPMOD) service that processes inbound traffic.

Use this URL to configure integration with Kaspersky Anti Targeted Attack Platform via ICAP on a proxy server that is used in your organization.

5. Click the **Apply** button.

Integration with a proxy server over the ICAP protocol will be enabled.

Configuring integration with a mail server via POP3

If you are using the distributed solution and multitenancy (see page 43) mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

► *To configure integration with a mail server via POP3:*

1. Select the **Sensor servers** section in the window of the program web interface.
The **Server list** table will be displayed.
2. Select the Sensor component for which you want to configure integration with the mail server via POP3.
A page with the Sensor component settings opens.
3. Select the **POP3 integration** section.
4. Set the toggle switch next to the **State** parameter to **Enabled**.
5. In the **Mail server** field, specify the IP address of the mail server with which you want to configure integration.
6. In the **Port** field, specify the port for connecting to the mail server.
7. In the **Receive every** field, specify the mail server connection frequency (in seconds).
8. If you want to use TLS encryption of connections with the mail server via POP3, select the **Use TLS encryption** check box.
9. In the **User name** field, specify the account name used for accessing the mail server.
10. In the **Password** field, specify the password for accessing the mail server.
11. Select one of the following options in the **TLS Certificate** drop-down list:
 - **Accept any.**
 - **Accept untrusted self-signed.**
 - **Accept only trusted.**

When establishing a connection with an external mail server, it is recommended to configure the acceptance of only trusted TLS certificates. If you accept untrusted TLS certificates, protection of the connection against MITM attacks cannot be guaranteed. Even though the acceptance of trusted TLS certificates also cannot guarantee protection of the connection against MITM attacks, it is the most secure of the supported methods for integration with a mail server over the POP3 protocol.

12. If necessary, in the **Cipher suite** field, modify the OpenSSL settings used when establishing a connection with the mail server via POP3.
You can view reference information on OpenSSL by clicking the **Help** link.
13. Click the **Apply** button.

Integration with the mail server via POP3 will be configured.

Managing the Endpoint Sensors component

The Endpoint Sensors component (see page [40](#)) is installed on separate computers (hereinafter referred to as “hosts”) that belong to the corporate IT infrastructure and run a Microsoft Windows operating system. Continuously monitors processes running on those computers, active network connections, and files that are modified.

Users with **Senior security officer**, **Security officer**, **Local administrator**, and **Administrator** roles can assess how regularly data is received from hosts on which the Endpoint Sensors component is installed, on the **Endpoint Sensors** tab of the program web interface window for organizations whose data the user is allowed to access (see page [160](#)). If you are using distributed solution and multitenancy mode, the web interface of the PCN server displays the list of Endpoint Sensors components for the PCN and all connected SCNs.

Users with the **Local administrator** and **Administrator** roles can configure the display of how regularly data is received from hosts with the Endpoint Sensors installed, for organizations whose data they are allowed to access (see page [160](#)).

If suspicious network activity is detected, users with the **Senior security officer** role can isolate (see page [291](#)) any host with the Endpoint Sensors component from the network, for organizations whose data the user is allowed to access (see page [160](#)). In this case, the connection between the server with the Central Node component and a host with the Endpoint Sensors component will not be interrupted.

For support in case of faulty operation of the Endpoint Sensors component, Technical Support experts may ask you to perform the following actions for debugging purposes (including in Technical Support Mode (see page [155](#))):

- Activate collection of extended diagnostic information.
- Modify the settings of individual program components.
- Modify the settings for storing and sending the obtained diagnostic information.
- Configure network traffic to be intercepted and saved to a file.

Technical Support experts will provide all the information needed to perform these operations (description of the sequence of steps, settings to be modified, configuration files, scripts, additional command line functionality, debugging modules, special-purpose utilities, etc.) and inform you about the scope of data gathered for debugging purposes. The extended diagnostic information that is gathered is saved on the user's computer. The collected data is not automatically sent to Kaspersky Lab.

The operations listed above should be performed only when instructed by and under the supervision of Technical Support experts. Unsupervised changes to program settings performed in ways other than those described in the Administrator's Guide or according to the instructions of Technical Support experts can slow down or crash the operating system, reduce computer security, or compromise the availability and integrity of data being processed.

Selecting an organization to manage in the Endpoint Sensors section

If you are using multitenancy mode, prior to using the **Endpoint Sensors** section you need to select the organization whose data you want to view.

► *To select an organization for managing in the **Endpoint Sensors** section:*

1. In the upper part of the program web interface menu, click the arrow next to the organization name.

2. In the drop-down list, select an organization.

Data for the selected organization is displayed. If you want to select a different organization, you need to repeat the organization selection procedure.

Viewing the Endpoint Sensors table on a standalone Central Node server

The table of hosts with the Endpoint Sensors component is located in the **Endpoint Sensors** section of the program web interface window.

If you are using a standalone Central Node server, but not using KSC integration, distributed solution and multitenancy mode, the host table with the Endpoint Sensors component can display the following data:

- **Host**—Host name with the Endpoint Sensors component.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Version**—Version of the Endpoint Sensors component installed.
- **Activity**—Activity indicator of the Endpoint Sensors component. Possible values:
 - **Normal activity** for hosts from which latest data was recently received.
 - **Warning** for hosts from which latest data was received a long time ago.
 - **Critical inactivity** for hosts from which latest data was received an extremely long time ago.

Clicking any column of the table opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

Viewing the Endpoint Sensors table on a standalone Central Node server with KSC integration

If you have configured integration with KSC, the table of hosts with the Endpoint Sensors component is located in the **Endpoint Sensors** section of the program web interface window.

The **Endpoint Sensors** section includes the following tabs:

- **Central Node.** Displays information about hosts with the Endpoint Sensors component that are connected to this Central Node server.
- **KSC.** Displays information about all hosts connected to KSC.

The **Central Node** tab can display the following information:

- **Host**—Host name with the Endpoint Sensors component.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Version**—Version of the Endpoint Sensors component installed.

- **Activity**—Activity indicator of the Endpoint Sensors component. Possible values:
 - **Normal activity** for hosts from which latest data was recently received.
 - **Warning** for hosts from which latest data was received a long time ago.
 - **Critical inactivity** for hosts from which latest data was received an extremely long time ago.

The **KSC** tab can display the following information:

- **Host**—Host name with the Endpoint Sensors component.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Endpoint Sensor**—Type of component used as an Endpoint Sensors component.

A component may be one of the following types:

- **Endpoint Sensor.**

The Endpoint Sensors component (see page [40](#)) that was installed from the Kaspersky Anti Targeted Attack Platform package.

- **Built-in KES.**

The Endpoint Sensors component that is included in Kaspersky Endpoint Security for Windows.

- **Version**— version of the Endpoint Sensors component installed.
- **Server**—Name of the server with the Central Node component.
- **Sensor state**—Status of the Endpoint Sensors component installed on the computer.

An Endpoint Sensors component can have one of the following statuses:

- **Running.**
- **Stopped.**
- **Failure.**
- **Not installed.**

- **Host state**—Host status of the computer with the Endpoint Sensors component.

A host can have one of the following states:

- **Offline**
- **Online**

- **Errors**—Error status in the operation of the Endpoint Sensors component. The status can take the value **No errors** or can contain information about the type of error in the operation of the Endpoint Sensors component.

Clicking any column of the table opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

By clicking the link with the IP address of the computer where the Endpoint Sensors component is installed, you can also choose the **Navigate to alerts filtered by this value** action.

Clicking the link with the name of the host on which the Endpoint Sensors is installed allows you to select the following actions:

- **Isolate from network.**
- **Find events.**
- **Find alerts.**

Viewing the Endpoint Sensors table in distributed solution and multitenancy mode

The table of hosts with the Endpoint Sensors component is located in the **Endpoint Sensors** section of the program web interface window.

If you are using the distributed solution and multitenancy mode, but are not using integration with KSC, the table contains information about the Endpoint Sensors components connected to the PCN and all SCN servers. The table can display the following data:

- **Host**—Host name with the Endpoint Sensors component.
Clicking the link with the host name opens a list in which you can select one of the following actions:
 - **Filter by this value.**
 - **Exclude from filter.**
 - **New prevention rule.**
 - **Find events.**
 - **Find alerts.**
 - **Copy value to clipboard.**
- **Servers**—Names of servers to which the host with the Endpoint Sensors is connected.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Version**—Version of the Endpoint Sensors component installed.
- **Activity**—Activity indicator of the Endpoint Sensors component. Possible values:
 - **Normal activity** for hosts from which latest data was recently received.
 - **Warning** for hosts from which latest data was received a long time ago.
 - **Critical inactivity** for hosts from which latest data was received an extremely long time ago.

Clicking any column of the table opens a list in which you can select one of the following actions:

- **Filter by this value.**

- **Exclude from filter.**
- **Copy value to clipboard.**

By clicking the link with the IP address of the computer where the Endpoint Sensors component is installed, you can also choose the **Navigate to alerts filtered by this value** action.

Viewing information about a host

► *To view information about a host with the Endpoint Sensors component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Select the host for which you want to view information.

This opens a window containing information about the host.



The window contains the following information:

- **State**—Host status of the host with the Endpoint Sensors component.
A host can have one of the following states:
 - **Online**
 - **Offline**
- **Host**—Host name of the computer with the Endpoint Sensors component.
To perform the **Copy value to clipboard** action, click the link with the host name.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system on the computer with the Endpoint Sensors component installed.
- **Protection**—Host status with the Endpoint Sensors component.
- **Server**—Name of the SCN or PCN server. Only displayed in distributed solution and multitenancy mode.
- **Server name**—Name of the Central Node server.
- **Last connection**—time of the last connection to the Central Node, SCN, or PCN server.
- **Version**—Type and version of the Endpoint Sensors component installed.
- **Status**—Status of the Endpoint Sensors component.

Filtering and searching Endpoint Sensors by host name

► *To filter or search for hosts with the Endpoint Sensors component by host name:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.

2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Host** link to open the filter configuration window.
4. If you want to display only isolated hosts, select the **Show isolated Endpoint Sensors only** check box.
5. In the drop-down list, select one of the following filtering operators:
 - **Contains.**
 - **Does not contain.**
6. In the entry field, specify one or several characters of the host name.
7. To add a filter condition using a different criterion, click  and specify the filter condition.
8. If you want to delete the filter condition, click the  button to the right of the field.
9. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors that have been isolated from the network

- *To filter or search for hosts with the Endpoint Sensors component that are isolated from the network (see page [291](#)):*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Host** link to open the filter configuration window.
4. Select the **Show isolated Endpoint Sensors only** check box.
5. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by PCN and SCN server names

If you are using distributed solution and multitenancy mode, you can filter or find hosts with the Endpoint Sensors component based on the names of PCN and SCN servers to which those hosts are connected.

► *To filter or search for hosts with the Endpoint Sensors component by the names of PCN and SCN servers:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. Click the **Servers** link to open the filter configuration window.
3. Select check boxes next to names of servers by which you want to filter or search for hosts with the Endpoint Sensors component.
4. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by computer IP address


► *To filter or search for hosts with the Endpoint Sensors component based on the IP address of the computer with the Endpoint Sensors component installed:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **IP** link to open the filter configuration window.
4. In the drop-down list, select one of the following filtering operators:
 - **Contains.**

- **Does not contain.**

5. In the entry field, specify one or several characters of the computer IP address. You can enter the IP address or subnet mask in IPv4 format (for example, 192.0.0.1 or 192.0.0.0/16).

6. To add a filter condition using a different criterion, click  and specify the filter condition.

7. If you want to delete the filter condition, click the  button to the right of the field.

8. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by operating system version on the computer

► *To filter or search for hosts with the Endpoint Sensors component based on the version of the operating system installed on the computer hosting the Endpoint Sensors component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.

This will open the table of hosts with the Endpoint Sensors component.

2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:

- **Central Node.**
- **KSC.**


3. Click the **OS** link to open the filter configuration window.

4. In the drop-down list, select one of the following filtering operators:

- **Contains.**
- **Does not contain.**

5. In the entry field, specify one or several characters of the operating system version.

6. To add a filter condition using a different criterion, click  and specify the filter condition.

7. If you want to delete the filter condition, click the  button to the right of the field.

8. Click the **Apply** button.



The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors based on the Endpoint Sensor component version

► *To filter or search for hosts with the Endpoint Sensors component based on the version of the Endpoint Sensors component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Version** link to open the filter configuration window.
4. In the drop-down list, select one of the following filtering operators:
 - **Contains.**
 - **Does not contain.**
5. In the entry field, specify one or several characters of the version of the Endpoint Sensors component.
6. To add a filter condition using a different criterion, click  and specify the filter condition.
7. If you want to delete the filter condition, click the  button to the right of the field.
8. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors based on their activity

► *To filter or search for the Endpoint Sensors components based on their activity:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.

2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Activity** link to open the filter configuration window.
4. Select the check boxes next to one or more Endpoint Sensors component activity indicators (see page [209](#)):
 - **Normal activity**, if you want to find hosts from which the last data was recently received.
 - **Warning**, if you want to find hosts from which the last data was received a long time ago.
 - **Critical inactivity**, if you want to find hosts from which the last data was received an extremely long time ago.
5. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Quickly creating a filter for computers with the Endpoint Sensors component

► *To quickly create a filter for hosts with the Endpoint Sensors component:*


1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Do the following to quickly add filter conditions to the filter being created:
 - a. Position the mouse cursor on the link containing the table column value that you want to add as a filter condition.
 - b. Left-click it.
This opens a list of actions to perform on the value.
 - c. In the list that opens, select one of the following actions:
 - **Filter by this value**, if you want to include this value in the filter condition.
 - **Exclude from filter**, if you want to exclude the value from the filter condition.

4. If you want to add several filter conditions to the filter being created, perform the actions to quickly add each filter condition to the filter being created.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

Clearing the Endpoint Sensors filter

► *To clear a filter for hosts with the Endpoint Sensors component based on one or multiple filter conditions:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the  button on the right of the header of the table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

Configuring Endpoint Sensors activity indicators

Users with the **Local administrator** and **Administrator** permissions can define which period of inactivity of computers with the Endpoint Sensors component is considered to be normal, low, or very low activity, and can configure the activity indicators for Endpoint Sensors components. All users can view the activity indicators for Endpoint Sensors.

► *To configure activity indicators for Endpoint Sensors components:*

1. Sign in to the program web interface under the **Local administrator** or **Administrator** account.
2. In the window of the program web interface, select the **Settings** section, **Endpoint Sensors** subsection.
3. In the fields under the section name, enter the number of days of inactivity of computers with the Endpoint Sensors component that you want to display as **Warning** and **Critical inactivity**.
4. Click the **Apply** button.

Users with **Senior security officer** and **Security officer** permissions can see activity indicators that you configured for Endpoint Sensors components in the **Activity** field of the Endpoint Sensors host table in the **Endpoint Sensors** section of the program web interface.

Creating a task for restarting the Endpoint Sensors components in KSC

You can create a group task for restarting Endpoint Sensors components on all computers in the Kaspersky Security Center Administration Console. If program integration with Kaspersky Security Center is not configured, you can use a Windows group policy to restart components. For more details on group policies, please refer to the documentation on the operating system.

► *To create a group task for restarting Endpoint Sensors components:*

1. Open the Kaspersky Security Center Administration Console.
2. In the folder containing the managed devices of the Administration Console tree, select the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the tab with the list of tasks.
4. Click the task creation button.
The New Task Wizard starts.
5. In the task type selection window, choose to start or stop the program.
6. Follow the instructions of the New Task Wizard.

The task for restarting the Endpoint Sensors components service will be created. For more details about group tasks and about starting tasks, please refer to the Kaspersky Security Center Help Guide

<https://help.kaspersky.com/KSC/SP3/en-US/5022.htm>.

Configuring integration with the Sandbox component

You can connect one Sandbox component to multiple Central Node components.

The following procedure is used to configure the Sandbox component connection with the Central Node component:

a. Creating a request to connect to the Sandbox component

You can create a request in the administrator menu (see page [168](#)) or in the program web interface (see page [211](#)) under an administrator account. You must create a request for each server with the Central Node component that you want to connect to the Sandbox component.

b. Processing a connection request (see page [169](#)) in the Sandbox web interface

You can accept or reject each request.

Viewing the table of servers with the Sandbox component

The table of servers with the Sandbox component is located on the **Sandbox servers** tab of the program web interface window.

The table contains the following information:

- **IP and name**—IP address or fully qualified domain name of the server with the Sandbox component.
- **Certificate fingerprint**—Certificate fingerprint of the server with the Sandbox component.
- **Authorization**—Status of the request to connect to the Sandbox component.
- **Status**—Status of the connection to the Sandbox component.

Creating a request to connect to the server with the Sandbox component

► *To create a request to connect to the server with the Sandbox component through the program web interface:*

1. Select the **Sandbox servers** section in the window of the program web interface.
2. In the upper-right corner of the window, click the **Add** button.

The **Sandbox connection** window opens.

3. In the **IP** field, specify the IP address of the server with the Sandbox component to which you want to connect.
4. Click **Get certificate fingerprint**.

The workspace displays the fingerprint of the certificate of the server with the Sandbox component.

5. Compare the obtained certificate fingerprint with the fingerprint indicated in the Sandbox web interface in the **KATA Authorization** section in the **Certificate fingerprint** field.

If the certificate fingerprints match, perform the next steps of the instructions.

If certificate fingerprints do not match, confirming the connection is not recommended. Make sure the data you entered is correct.

6. In the **Name** field, specify the Sandbox component name that will be displayed in the web interface of the Central Node component.

This name is not related to the name of the host where the Sandbox is installed.

7. If you want to activate a connection with Sandbox immediately after connecting, select the **Enable** check box.
8. Click the **Add** button.

The connection request is displayed in the web interface of the Sandbox component.

Enabling and disabling a connection with the Sandbox component

► *To activate a connection with the Sandbox component or to disable it:*

1. Select the **Sandbox servers** section in the window of the program web interface.
The table of servers with Sandbox components is displayed.
2. In the line containing the relevant server in the **Status** column, perform one of the following actions:
 - If you want to activate a connection with the Sandbox component, set the toggle switch to **Enabled**.
 - If you want to disable a connection with the Sandbox component, set the toggle switch to **Disabled**.
3. Click the **Apply** button.

The connection with the Sandbox component will become active or will be disabled.

Deleting a connection with the Sandbox component

► *To delete a connection with the Sandbox component:*

1. Select the **Sandbox servers** section in the window of the program web interface.
This displays the table of computers on which the Sandbox component is installed.
2. Select the check box in the line containing the Sandbox component whose connection you want to delete.
3. In the upper-right corner of the window, click the **Delete** button.
4. In the confirmation window, click **Yes**.

The connection with the Sandbox component will be deleted.

Configuring integration with external systems

You can configure integration of Kaspersky Anti Targeted Attack Platform with external systems to scan files stored in those systems. Their scan results will be displayed in the alerts table (see page [236](#)).

The role of an external system can be served by a mail sensor, such as Kaspersky Secure Mail Gateway or Kaspersky Security for Linux Mail Server. The mail sensor sends email messages to Kaspersky Anti Targeted Attack Platform for processing. Based on the results of processing of email messages in Kaspersky Anti Targeted Attack Platform, the mail sensor may block the transfer of messages.

Integration of Kaspersky Anti Targeted Attack Platform with external systems involves the following procedure:

a. Enter the integration settings and create an integration request from the external system.

For more details about entering integration settings for the mail sensor, please refer to the Kaspersky Secure Mail Gateway Help Guide <https://help.kaspersky.com/KSMG/1.1.2/en-US/100512.htm> or the Kaspersky Security for Linux Mail Server Help Guide <https://help.kaspersky.com/KLMS/8.2/en-US/100512.htm>.

To integrate other external systems, use the REST API.

b. Confirm integration for Kaspersky Anti Targeted Attack Platform (see page [214](#))

External systems may use identical IDs and certificates for authorization on the server with the Central Node component. If this is the case, a single integration request will be displayed in the interface of Kaspersky Anti Targeted Attack Platform.

c. Check the connection between the external system and Kaspersky Anti Targeted Attack Platform

Viewing the table of external systems

The table of external systems is in the **External systems** section of the program web interface window. The table contains the following information:

- **Sensor**—IP address or domain name of the external system server.
- **Type**—Type of external system (mail sensor or other system).
- **Name**—Name of the integrated external system that is not a mail sensor.
A dash is displayed in this column for a mail sensor.
- **ID**—ID of the external system.
- **Certificate fingerprint**—Fingerprint of the TLS certificate of the server with the external system used to establish an encrypted connection with the server hosting the Central Node component.

The certificate fingerprint of the server with the Central Node component is displayed in the upper part of the window in the **Certificate fingerprint** field.

- **State**—State of the integration request.

Processing a request from an external system

► *To process an integration request from an external system:*

1. Select the **External systems** section in the window of the program web interface.

The **Server list** table displays the already connected external systems, and requests for integration with Kaspersky Anti Targeted Attack Platform from external systems.

2. In the line containing the integration request, perform one of the following actions:
 - If you want to configure integration with the external system, click the **Accept** button.
 - If you do not want to configure integration with the external system, click the **Reject** button.
3. In the confirmation window, click **Yes**.

The integration request from the external system will be processed.

Removing an external system from the list of those allowed to integrate

After you have accepted an integration request from an external system, you can remove it from the list of those allowed to integrate. If this is the case, the connection between Kaspersky Anti Targeted Attack Platform and the external system will be terminated.

► *To remove an external system from the list of those allowed to integrate:*

1. Select the **External systems** section in the window of the program web interface.

The **Server list** list displays the already added external systems and the requests to integrate with Kaspersky Anti Targeted Attack Platform from external systems.

2. Click the **Delete** button in the line containing the integration request from the external system that you want to remove.
3. In the confirmation window, click **Yes**.

The external system will be removed from the list of those allowed to integrate.

Configuring the priority for processing traffic from mail sensors

You can enable or disable the maximum priority for processing traffic from mail sensors.

► *To enable or disable the maximum priority for processing traffic from mail sensors:*

1. Select the **External systems** section in the window of the program web interface.
2. Do one of the following:
 - Turn on the toggle switch next to the name of the **Process traffic with maximum priority** parameter if you want to enable the maximum priority for processing traffic from mail sensors.
 - Turn off the toggle switch next to the name of the **Process traffic with maximum priority** parameter if you want to disable the maximum priority for processing traffic from mail sensors.

The priority for processing traffic from mail sensors will be configured.

Configuring integration with an SIEM system

Kaspersky Anti Targeted Attack Platform can publish alerts to a *SIEM system* already in use at your organization using the Syslog protocol.

You can use TLS encryption for data transmission.

Enabling and disabling event logging to a local log

You can configure event logging to the local log saved on the computer with the Central Node component. The file of this log can be imported into a SIEM system whose integration with the program has not been configured.

► *To enable or disable event logging to a local log:*

1. In the window of the program web interface, select the **Settings** section, **SIEM System** subsection.
2. Do one of the following:
 - Turn on the toggle switch next to the name of the **Local Log** parameter if you want to enable event logging to a local log.
 - Turn off the toggle switch next to the name of the **Local Log** parameter if you want to disable event logging to a local log.
3. Click **Apply** in the lower part of the window.

Event logging to the local log will be enabled or disabled.

Enabling and disabling event logging to a remote log

The remote log is saved on the server on which a SIEM system is installed. The settings of integration with the SIEM system (see page [215](#)) must be configured to write to the remote log.

► *To enable or disable event logging to a remote log:*

1. In the window of the program web interface, select the **Settings** section, **SIEM System** subsection.
2. Do one of the following:
 - Turn on the toggle switch next to the name of the **Remote Log** parameter, if you want to enable event logging to a remote log.
 - Turn off the toggle switch next to the name of the **Remote Log** parameter, if you want to disable event logging to a remote log.
3. Click **Apply** in the lower part of the window.

Configuring the main settings for SIEM system integration

► *To configure the main settings for SIEM system integration:*

1. In the window of the program web interface, select the **Settings** section, **SIEM System** subsection.
2. Turn on the toggle switch next to the name of the **Remote Log** parameter if it is turned off.
3. In the **Host/IP** field, enter the IP address or host name of the server of your SIEM system.
4. In the **Port** field, enter the port number used for connecting to your SIEM system.
5. In the **Protocol** field, select **TCP** or **UDP**.
6. In the **External device ID** field, specify the ID of the device on which your SIEM system is installed.
7. In the **Heartbeat** field, enter the interval for sending messages to the SIEM system about the status of Kaspersky Anti Targeted Attack Platform components.

8. Click **Apply** in the lower part of the window.

The main settings of integration with the SIEM system will be configured.

Enabling and disabling TLS encryption of the connection with the SIEM system

► *To enable or disable TLS encryption of the connection with the SIEM system:*

1. In the window of the program web interface, select the **Settings** section, **SIEM System** subsection.
2. Turn on the toggle switch next to the name of the **Remote Log** parameter if it is turned off.
3. In the **TLS encryption** section, perform one of the following actions:
 - Turn on the toggle switch next to the name of the **TLS encryption** parameter if you want to enable TLS encryption of the connection with the SIEM system.
 - Turn off the toggle switch next to the name of the **TLS encryption** parameter if you want to disable TLS encryption of the connection with the SIEM system.

The toggle switch next to the name of the **TLS encryption** parameter is available only if a TLS certificate is loaded.

4. Click **Apply** in the lower part of the window.

TLS encryption of the connection with the SIEM system will be enabled or disabled.

Loading a TLS certificate

► *To load a TLS certificate for encrypting the connection with the SIEM system:*

1. In the window of the program web interface, select the **Settings** section, **SIEM System** subsection.
2. Turn on the toggle switch next to the name of the **Remote Log** parameter if it is turned off.
3. In the **TLS encryption** section, click the **Upload** button.
The file selection window opens.
4. Select a TLS certificate file to download and click the **Open** button.
The file selection window closes.
The TLS certificate will be added to the program.
5. Click **Apply** in the lower part of the window.

The uploaded TLS certificate will be used to encrypt the connection with the SIEM system.

Content and properties of syslog messages about alerts

Information about each alert is transmitted in a separate syslog category (syslog facility) that is not used by the system to deliver messages from other sources. Information about each alert is transmitted as a separate syslog message in CEF format. If the alert was generated by the Targeted Attack Analyzer module, information about that alert is transmitted as multiple separate syslog messages in CEF format.

The default maximum size of a syslog message about an alert is 32 KB. Messages that exceed the maximum size are truncated at the end.

The header of each syslog message about an alert contains the following information:

- Format version.
Current version number: 0. Current field value: CEF:0.
- Vendor.

Current field value: AO Kaspersky Lab.

- Program name.

Current field value: Kaspersky Anti Targeted Attack Platform.

- Program version.

Current field value: 3.6.

- Alert type.

See the table below.

- Event name.

See the table below.

- Alert importance.

Allowed field values: Low, Medium, High or 0 (for heartbeat messages).

- Additional information.

Example:

```
CEF:0|AO Kaspersky Lab| Kaspersky Anti Targeted Attack Platform
|3.6|url_web| URL from web detected|Low|
```

The body of a syslog message about an alert matches the information about that alert that is displayed in the program web interface. All fields are presented in the format "<key>=<value>". Depending on whether the alert occurred in network traffic or mail traffic, and depending on the technology that generated the alert, various keys may be transmitted in the body of a syslog message. If the value is empty, the key is not transmitted.

The keys, as well as their values contained in a message, are presented in the table below.

Alert type	Alert name and description	Key and description of its value
file_web	File from web detected A file was detected in network traffic.	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>dst</code> = <destination IP address>. • <code>dpt</code> = <destination port>. • <code>src</code> = <source IP address>. • <code>spt</code> = <source port>. • <code>shost</code> = <name of the host on which the file was detected>. • <code>suser</code> = <user name>. • <code>fName</code> = <name of the file within the compound object>. • <code>fsize</code> = <size of the file within the compound object (in bytes)>. • <code>fileType</code> = <format of the file within the compound object>. • <code>fileHash</code> = <MD5 hash of the file within the compound object>. • <code>KasperskyLabKATAcompositeFilePath</code> = <name of the compound object>. • <code>KasperskyLabKATAcompositeFileSize</code> = <total size of the compound object (in bytes)>. • <code>KasperskyLabKATAcompositeFileHash</code> = <MD5 hash of the compound object>. • <code>KasperskyLabKATAfileSHA256</code> = <SHA256 hash of the compound object>. • <code>cs2</code> = <technology that was used to detect the file>. • <code>cs3Label</code> = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • <code>cs1</code> = <list of types of the detected objects according to the Kaspersky Lab classification>. • <code>cs3</code> = <version of databases used to scan the file>. • <code>app</code> = <name of the application-level protocol> (HTTP(S) or FTP). • <code>requestMethod</code> = <HTTP request method> (only for the HTTP(S) protocol). • <code>requestClientApplication</code> = <User Agent of the client computer> (only for the HTTP(S) protocol). • <code>request</code> = <URL of the detected object> (only for the HTTP(S) protocol). • <code>requestContext</code> = <HTTP Referer header> (only for the HTTP(S) protocol).

Alert type	Alert name and description	Key and description of its value
file_mail	File from mail detected A file was detected in mail traffic.	<ul style="list-style-type: none"> • eventId = <alert ID>. • rt = <date and time of alert>. • fName = <name of the file within the compound object>. • fsize = <size of the file within the compound object (in bytes)>. • fileType = <format of the file within the compound object>. • fileHash = <MD5 hash of the file within the compound object>. • KasperskyLabKATAcompositeFilePath = <name of the compound object>. • KasperskyLabKATAcompositeFileSize = <total size of the compound object (in bytes)>. • KasperskyLabKATAcompositeFileHash = <MD5 hash of the compound object>. • KasperskyLabKATAfileSHA256 = <SHA256 hash of the compound object>. • cs2 = <technology that was used to detect the file>. • cs3Label = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • cs1 = <list of types of the detected objects according to the Kaspersky Lab classification>. • cs3 = <version of databases used to scan the file>. • externalId = <Email message ID>. • suser = <email address of sender>. • duser = <email addresses of recipients>. • msg = <message subject>.

Table 12. Information about an alert in syslog messages

Alert type	Alert name and description	Key and description of its value
ids	IDS event detected An alert was generated by the Intrusion Detection System module.	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>requestMethod</code> = <HTTP request method> (only for the HTTP(S) protocol). • <code>requestClientApplication</code> = <User Agent of the client computer> (only for the HTTP(S) protocol). • <code>rt</code> = <date and time of alert>. • <code>dst</code> = <destination IP address>. • <code>dpt</code> = <destination port>. • <code>src</code> = <source IP address>. • <code>spt</code> = <source port>. • <code>proto</code> = <name of the network-level protocol> (TCP or UDP). • <code>cs1</code> = <type of the detected object according to the Kaspersky Lab classification>. • <code>cs2Label</code> = <name of the IDS rule>. • <code>cs2</code> = <number of the IDS rule>. • <code>cs3</code> = <Intrusion Detection System module database version>. • <code>requestMethod</code> = <HTTP request method> (only for the HTTP protocol). • <code>requestClientApplication</code> = <User Agent of the client computer> (only for the HTTP protocol). • <code>request</code> = <URL of the detected object>.
url_web	URL from web detected An alert was generated by URL Reputation technology in network traffic.	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>dst</code> = <destination IP address>. • <code>dpt</code> = <destination port>. • <code>src</code> = <source IP address>. • <code>spt</code> = <source port>. • <code>shost</code> = <name of the host on which the file was detected>. • <code>suser</code> = <user name>. • <code>cs1</code> = <list of categories to which the URL of the detected object belongs>. • <code>requestMethod</code> = <HTTP request method>. • <code>requestClientApplication</code> = <User Agent of the client computer>. • <code>request</code> = <URL of the detected object>. • <code>requestContext</code> = <HTTP Referer header>. • <code>reason</code> = <HTTP response code>.

Alert type	Alert name and description	Key and description of its value
url_mail	<p>URL from mail detected</p> <p>An alert was generated by URL Reputation technology in mail traffic.</p>	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>externalId</code> = <Email message ID>. • <code>suser</code> = <email address of sender>. • <code>duser</code> = <email addresses of recipients>. • <code>msg</code> = <message subject>. • <code>request</code> = <URL of the detected object>. • <code>cs2</code> = <technology that was used to generate the alert> (Sandbox or URL Reputation). • <code>cs3Label</code> = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • <code>cs1</code> = <list of types of the detected objects according to the Kaspersky Lab classification> (for the Sandbox component) or <list of categories> (for the URL Reputation technology). • <code>cs3</code> = <version of databases used to scan the file> (for the Sandbox component).
dns	<p>DNS request detected</p> <p>An alert was generated by URL Reputation technology in DNS traffic.</p>	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>dst</code> = <destination IP address>. • <code>dpt</code> = <destination port>. • <code>src</code> = <source IP address>. • <code>spt</code> = <source port>. • <code>shost</code> = <name of the host on which the file was detected>. • <code>suser</code> = <user name>. • <code>cs2</code> = <list of URL categories to which the domain names belong>. • <code>requestMethod</code> = <type of DNS message> (request or response). • <code>flexString1</code> = <type of record from the DNS request>. • <code>dhost</code> = <host name from the DNS request>. • <code>cs1</code> = <list of domain names from the DNS response>.

Alert type	Alert name and description	Key and description of its value
taa	<p>Suspicious process activity</p> <p>An alert was generated by Targeted Attack Analyzer technology. Suspicious process activity.</p>	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>src</code> = <source IP address>. • <code>shost</code> = <name of the host on which the file was detected>. • <code>fName</code> = <name of the file within the compound object>. • <code>fileHash</code> = <MD5 hash of the file within the compound object>. • <code>FilePath</code> = <path to the file on the computer with the Endpoint Sensors component>. • <code>KasperskyLabKATAfileSHA256</code> = <SHA256 hash of the compound object>. • <code>cs1</code> = <list of types of the detected objects according to the Kaspersky Lab classification>.
taa	<p>Suspicious remote host activity</p> <p>An alert was generated by Targeted Attack Analyzer technology. Suspicious remote host activity.</p>	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>src</code> = <source IP address>. • <code>shost</code> = <name of the host on which the file was detected>. • <code>dhost</code> = <name of the remote host>. • <code>cs1</code> = <list of types of the detected objects according to the Kaspersky Lab classification>.

Alert type	Alert name and description	Key and description of its value
file_endpoint	<p>File from endpoint detected</p> <p>An alert was generated by the Endpoint Sensors component on the user's computer and contains a file.</p>	<ul style="list-style-type: none"> • eventId = <alert ID>. • rt = <date and time of alert>. • src = <source IP address>. • shost = <name of the host on which the file was detected>. • fName = <name of the file within the compound object>. • fsize = <size of the file within the compound object (in bytes)>. • fileType = <format of the file within the compound object>. • fileHash = <MD5 hash of the file within the compound object>. • KasperskyLabKATAcompositeFilePath = <name of the compound object>. • KasperskyLabKATAcompositeFileSize = <total size of the compound object (in bytes)>. • KasperskyLabKATAcompositeFileHash = <MD5 hash of the compound object>. • KasperskyLabKATAfileSHA256 = <SHA256 hash of the compound object>. • cs2 = <technology that was used to detect the file>. • cs3Label = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • cs1 = <list of types of the detected objects according to the Kaspersky Lab classification>. • cs3 = <version of databases used to scan the file>. • app = <name of the application-level protocol> (HTTP(S) or FTP). • FilePath = <path to the file on the computer with the Endpoint Sensors component>.
iocScanningEP	<p>IOC has tripped on endpoint</p> <p>The alert was generated during an IOC scan of computers with the Endpoint Sensors component.</p> <p>This type of alert is available if you are using only KEDR functionality.</p>	<ul style="list-style-type: none"> • eventId = <alert ID>. • rt = <date and time of alert>. • src = <source IP address>. • shost = <name of the host on which the file was detected>. • cs1 = <name of the IOC file>.

Alert type	Alert name and description	Key and description of its value
iocScanning	<p>IOC has tripped on events database</p> <p>The alert was generated during an IOC scan of the events database.</p> <p>This type of alert is available if you are using only KEDR functionality.</p>	<ul style="list-style-type: none"> • <code>eventId</code> = <alert ID>. • <code>rt</code> = <date and time of alert>. • <code>shost</code> = <name of the host on which the file was detected>. • <code>cs1</code> = <name of the IOC file>.
heartbeat	<p>Periodic message containing the state of components.</p>	<ul style="list-style-type: none"> • <code>dvc</code> = <IP address of the server with the Central Node component>. • <code>rt</code> = <event date and time>. • <code>KasperskyLabKATAcomponentName</code> = <name of the component>. • <code>KasperskyLabKATAcomponentState</code> = <status of the component> (0 – OK, >0 – Error).

Configuring integration with Kaspersky Security Center

Integration with Kaspersky Security Center is not available in distributed solution mode (see page 43).

Using the program web interface, a user with the **Administrator** role can configure integration with Kaspersky Security Center and receive statistics on the operation of the Endpoint Sensors component.

To integrate with Kaspersky Security Center, you must create a user account in Kaspersky Security Center.

► *To configure the necessary permissions for a user account:*

1. Open the KSC Console.
2. Open the properties window of the relevant Administration Server.
3. In the left part of the server properties window, select the section containing security settings.
4. In the right part of the server properties window, select the user account whose permissions you want to configure.
5. Grant the user permissions to perform the following actions:
 - a. Read and modify – in the general functionality node in the basic functionality folder.
 - b. Read and execute – in the general functionality node in the Administration Server operations folder.
 - c. Read and create tunnels – in the system control node in the connections folder.
6. Save the changes.

For detailed information on working in Kaspersky Security Center, please refer to the *Kaspersky Security Center Help Guide*.

Enabling and disabling integration with Kaspersky Security Center

Integration with Kaspersky Security Center is not available in distributed solution mode (see page 43).

► *To enable or disable integration with Kaspersky Security Center:*

1. In the window of the program web interface, select the **Settings** section, **Kaspersky Security Center Integration** subsection.
2. Do one of the following:
 - Turn on the toggle switch next to the name of the **Integration** parameter if you want to enable integration with Kaspersky Security Center.
Integration with Kaspersky Security Center will be enabled.
 - Turn off the toggle switch next to the name of the **Integration** parameter if you want to disable integration with Kaspersky Security Center.
Integration with Kaspersky Security Center will be disabled.

Configuring the settings for integration with Kaspersky Security Center

Integration with Kaspersky Security Center is not available in distributed solution mode (see page 43).

► *To configure the settings for integration with Kaspersky Security Center:*

1. In the window of the program web interface, select the **Settings** section, **Kaspersky Security Center Integration** subsection.
2. Turn on the toggle switch next to the name of the **Integration** parameter if it is turned off.
3. In the **Host/IP** field, enter the IP address of Kaspersky Security Center.
4. In the **Port** field, enter the port used for connecting to Kaspersky Security Center.
5. In the **KSC Login** field, enter the user name with Kaspersky Security Center administrator permissions.
6. In the **KSC Password** field, enter the password for accessing Kaspersky Security Center.
7. Click **Apply** in the lower part of the window.

The settings for integration with Kaspersky Security Center will be configured.

Configuring server settings for delivery of notifications

The program can send notifications about alerts. To do so, you must configure the settings of the server used for sending notifications.

► *To configure the server settings for sending notifications:*

1. In the window of the program web interface, select the **Settings** section, **Mail notification server** subsection.
2. In the **Host** field, specify the IP address of the mail server.
3. In the **Port** field, specify the port for connecting to the mail server.
4. In the **Email from** field, specify the email address from which the notifications will be sent.
5. If you want to enable authentication on the mail server, select the **Use SMTP authentication of message recipients** check box.
6. In the **User name** field, specify the user name for authentication on the server used for sending notifications.
7. In the **Password** field, specify the password for authentication on the server used for sending notifications.
8. If you want to use TLS encryption when sending notifications, select the **Use TLS encryption** check box.
9. If you want to validate the certificate of the mail server, select the **Validate TLS encryption** check box.

The **Certificate fingerprint** field displays the fingerprint of the mail server certificate.

If the **Validate TLS encryption** check box is not selected, the program will consider any certificate of the mail server as trusted.

10. Click the **Apply** button.

The settings of the server used for sending notifications will be configured.

About database updates

Program databases ("databases") are files with records used by the program components and modules to detect events occurring in your organization's IT infrastructure.

Virus analysts at Kaspersky Lab detect hundreds of new threats daily (including "zero-day" exploits), create records to identify them, and include them in database updates packages ("update packages"). *Update packages* consist of one or more files containing records to identify threats that were detected since the previous update package was released. We recommend that you regularly receive update packages. When the program is installed, the database release date is the same as the program release date, and therefore you must update the databases immediately after installing the program.

The program periodically automatically checks for new update packages on the Kaspersky Lab update servers (once every 30 minutes). By default, if for some reason program databases are not updated for 24 hours, Kaspersky Anti Targeted Attack Platform displays this information in the **Dashboard** section of the window of the program web interface.

Selecting a database update source

You can select the source from which the program will download database updates. The update source may be the Kaspersky Lab server, or a network folder or local folder on one of the computers of your organization.

► *To select the source of program database updates:*

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Database update** section, in the **Update source** drop-down list, select one of the following values:
 - **Kaspersky Lab servers.**
 - **Custom URL.**
3. If you selected **Custom URL**, in the field under the drop-down list, specify the network path to the folder in which the program database updates will be saved.
4. Click the **Apply** button.

The program database update source will be applied.

Updating databases manually

► *To manually start a program database update:*

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Database update** section, click the **Start** button.

The program database update will be started. The progress of the update will be displayed to the right of the button.

Creating a list of passwords for archives

The program does not scan password-protected archives. You can create a list of the most frequently encountered passwords for archives that are used when exchanging files within your organization. If you do so, the program will try the passwords from the list when scanning an archive. If one of the passwords match, the archive will be unlocked and scanned.

The list of passwords defined in the program settings is also transmitted to the server with the Sandbox component.

► *To create a list of passwords for archives:*

1. In the window of the program web interface, select the **Settings** section, **Passwords to archives** subsection.
2. In the **Passwords to archives** field, enter the passwords that the program will use for password-protected archives.

Enter each password on a new line. You can enter up to 50 passwords.

3. Click the **Apply** button.

The list of passwords for archives will be created. When scanning PDF files and files of Microsoft Word, Excel, and PowerPoint that are password protected, the program will use the passwords from the defined list.

For a security officer: Getting started with the program web interface

This section is intended for specialists who are in charge of providing data security within an organization. It contains information and instructions on configuring resources for the security of a corporate IT infrastructure and timely detection of threats.

The program allows the joint work of several security officers.

Kaspersky Anti Targeted Attack Platform Interface

The program is managed through the web interface. Sections of the program web interface differ depending on the role of the user: **Administrator** or **Senior security officer** / **Security officer** (see page [229](#)).

The window of the program web interface contains the following items:

- Sections in the left part and in the lower part of the program web interface window.
- Tabs in the upper part of the program web interface window for certain sections of the program.
- The workspace in the lower part of the program web interface window.

Sections of the program web interface window

The program web interface that is available to users with the **Senior security officer** and **Security officer** roles provides the following sections:

- **Dashboard.** Contains Kaspersky Anti Targeted Attack Platform Monitoring data.
- **Alerts.** Contains information about alerts in your organization's network.
- **Threat Hunting.** Contains information about events detected on hosts of your organization.
- **Tasks.** Contains information about tasks that you can use to manage files and applications on hosts.
- **Prevention.** Contains information about policies that you can use to manage preventions of files running on selected hosts.
- **IOC/IOA Analysis.** Contains information about IOA analysis of events and alerts, IOC scanning of events, working with IOC files and the IOA white list.
- **Storage.** Contains information about managing objects in Backup and in Quarantine.
- **Endpoint Sensors.** Contains information about managing the Endpoint Sensors component and viewing data.
- **Reports.** Contains a report builder and a list of generated reports about alerts.
- **Settings** Contains information on the IOC scan schedule, and the settings for publishing objects in KPSN and assigning the VIP status to alerts based on information contained in alerts, YARA rules, the white list, passwords of archives, and added keys.

Workspace of the program web interface window

The workspace displays the information you choose to view in the sections and on the tabs of the program web interface window. It also contains control elements that you can use to configure how the information is displayed.

Selecting an organization to manage in the web interface of the program

If you are using multitenancy mode, you need to select the organization that you want to manage before using the web interface of the program.

► *To select an organization to manage in the web interface of the program:*

1. In the upper part of the program web interface menu, click the arrow next to the organization name.
2. In the **Select company** drop-down list, select an organization.

You can also type characters of the organization name in the search string and select the organization from the list of search results.

All actions in the program web interface are applied to the selected organization. If you want to select a different organization, you need to repeat the organization selection procedure.

Monitoring program operation

You can monitor program operation using the widgets in the **Dashboard** section of the program web interface window. You can add, delete and move widgets, configure the scale of widgets, and select the data display period.

About widgets and layouts

You can use widgets to monitor program operation.

The *layout* is the appearance of the workspace of the program web interface window in the **Dashboard** section. You can add, delete, and move widgets on the layout, and configure the scale of widgets.

If you are using the distributed solution and multitenancy mode, the section displays data on the organization that you chose (see page [230](#)).

By default, this section displays information only on alerts that were not processed by users. To also display information on processed alerts, turn on the **Processed** switch in the upper-right corner of the window.

The **Dashboard** section displays the following widgets:

- Alerts:
 - **Alerts by attack vector.** Displays detected objects based on the vector of the attack.
 - **Alerts by importance.** Displays the importance of alerts for users of the Kaspersky Anti Targeted Attack Platform depending on the impact that these alerts may have on the security of computers or the corporate LAN based on Kaspersky Lab experience.
 - **Alerts by status.** Displays the alert status depending on the Kaspersky Anti Targeted Attack Platform user processing the alert and on whether or not this alert has been processed.
 - **Alerts by technology.** Displays the names of the program modules or components that generated the alert.
 - **VIP Alerts by Importance.** Displays the importance of alerts with VIP status depending on the impact that these alerts may have on the security of computers or the corporate LAN based on Kaspersky Lab experience.

The left part of each widget displays attack vectors, alert importance levels, alert states, and technologies that generated the alerts. The right part of each widget displays the number of times that the program detected them during the selected period of data display on widgets (see page [182](#)).

To go to the **Alerts** section of the program web interface and view related alerts, click the link with the name of the attack vector, alert importance level, and technology that generated the alert. Alerts will be filtered based on the selected element.


- Top 10:
 - **Top 10 domains.** 10 domains most frequently seen in alerts.
 - **Top 10 email recipients.** 10 email recipients most frequently seen in alerts.
 - **Top 10 IP.** 10 IP addresses most frequently seen in alerts.
 - **Top 10 email senders.** 10 email senders most frequently seen in alerts.
 - **Top 10 IOA hosts.** 10 most frequently encountered hosts in IOA analysis events.
 - **Top 10 IOA rules.** 10 IOA rules that found the most events.

The left part of each widget lists the domains, addresses of recipients, IP addresses, and addresses of message senders, host names, and IOA rule names. The right part of each widget displays the number of times that the program detected them during the selected period of data display on widgets(see page [182](#)).

By clicking the link with the name of each domain, recipient address, IP address, message sender address, host name, and IOA rule name, you can go to the **Alerts** section of the program web interface and view related alerts. Alerts will be filtered based on the selected element.

Adding a widget to the current layout


► *To add a widget to the current layout:*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.
3. In the drop-down list, select **Customize**.
4. Click the **Widgets** button.
5. In the **Manage widgets** window that opens, turn on the toggle switch next to the widget that you want to add.

The widget will be added to the current layout.

Moving a widget in the current layout


► *To move a widget in the current layout:*


1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.
3. In the drop-down list, select **Customize**.
4. Select the widget that you want to move within the layout.
5. Left-click and hold down the left mouse button on the upper part of the widget to drag the widget to another place on the layout.
6. Click the **Save** button.

The current layout will be saved.

Removing a widget from the current layout


► *To remove a widget from the current layout:*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.

3. In the drop-down list, select **Customize**.
4. Click the  icon in the upper right corner of the widget that you want to remove from the layout.
The widget will be removed from the workspace of the program web interface window.
5. Click the **Save** button.
The widget will be removed from the current layout.

Saving a layout to PDF

► To save a layout to PDF:

1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.
3. In the drop-down list, select **Save as PDF**.
This opens the **Saving as PDF** window.
4. In the lower part of the window, in the **Layout** drop-down list, select the page orientation.
5. Click the **Download** button.
The layout in PDF format will be saved to the hard drive of your computer in the downloads folder of the browser.
6. Click the **Close** button.

Configuring the period for displaying data in widgets

You can configure the display of data on widgets for the following periods:

- **Day**
- **Week**
- **Month**

► To configure the display of data on widgets for a 24-hour period (from 00:00 to 23:59):

1. Select the **Dashboard** section in the program web interface window.
2. In the upper-right corner of the program web interface window, in the drop-down list of data display periods, select **Day**.
3. In the calendar to the right of the **Day** period name, select the date for which you want to obtain data on the widget.

All widgets on the **Dashboard** page display data for the period you selected.

► To configure the display of data on widgets for a week (Monday through Sunday):

1. Select the **Dashboard** section in the program web interface window.

2. In the upper-right corner of the program web interface window, in the drop-down list of data display periods, select **Week**.
3. In the calendar to the right of the **Week** period name, select the week for which you want to obtain data on the widget.


All widgets on the **Dashboard** page display data for the period you selected.

► *To configure the display of monthly data (calendar month) on widgets:*



1. Select the **Dashboard** section in the program web interface window.
2. In the upper-right corner of the program web interface window, in the drop-down list of data display periods, select **Month**.
3. In the calendar to the right of the **Month** period name, select the month for which you want to obtain data on the widget.

All widgets on the **Dashboard** page display data for the period you selected.

Configuring the widget display size

You can configure the display size for "Alerts" widgets. The  icon is located in the upper right corner of the widgets whose display size you can configure.

► *To configure the display size for widgets:*

1. Select the **Dashboard** section in the program web interface window.
2. In the upper part of the window, click the  button.
3. In the drop-down list, select **Customize**.
4. Click the  icon in the upper right corner of the widget.
5. In the drop-down list, select one of the following widget display sizes:

- **1x1.**
- **2x1.**
- **3x1.**

The display size of the selected widget will be changed.

6. Repeat these actions for all widgets whose display size you want to change.
7. Click the **Save** button.

The display size of widgets will be configured.

Main principles of working with "Alerts" widgets

You can configure the display size (see page [234](#)) for all "Alerts" widgets.

The left part of each widget displays the key of colors used on widgets.

Example:

The **Alerts by importance** widget displays the number of alerts of varying severity.

Importance—Alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer or corporate LAN security based on Kaspersky Lab experience.

On the **Alerts by importance** widget, alert importance is indicated with the following colors:

- Red—Alert has a high level of importance.
- Orange—Alert has a medium level of importance.
- Green—Alert has a low level of importance.

To the right of the color key is the number of alerts of each type for the selected period of data display on widgets (see page [182](#)).

By clicking the link with the type of each alert, you can go to the **Alerts** section of the program web interface and view all alerts of this type. Alerts will be filtered based on the specific type.

Example:

The **Alerts by attack vector** widget displays **Files from email** alerts, which indicate the number of files that Kaspersky Anti Targeted Attack Platform detected in mail traffic for the selected period of data display on widgets (see page [182](#)).

Clicking the **Files from email** link opens the **Alerts** section and displays all alerts associated with the detection of files in mail traffic for the selected period of data display on widgets. Data will be filtered based on the following parameters: **Time**, **Object type**=FILE and **Object source**=MAIL.

The right part of each widget displays data columns. The vertical axis shows the number of events, and the horizontal axis shows the date and time of the alert. You can edit the period of data display in widgets (see page [182](#)) and select the organization (see page [230](#)) for which information is displayed in the widget.

Position your mouse cursor on each data column to display the number of alerts counted for the period represented by the specific column. The number of unprocessed alerts is displayed by default. You can enable the display of processed alerts by selecting the **Processed** check box in the upper-right corner of the window. In this case, the total number of all alerts will be displayed.

Table of alerts

Kaspersky Anti Targeted Attack Platform processes data from the following sources:

- Mirrored traffic on the corporate LAN (HTTP, FTP, and DNS protocols).
- HTTP and FTP traffic, as well as HTTPS traffic if the administrator has configured SSL certificate replacement on the proxy server.
- Copies of email messages received via the POP3 or SMTP protocol, as well as copies of email messages received from Kaspersky Secure Mail Gateway or Kaspersky Security for Linux Mail Server if they are being used in your organization.
- Information on running processes, active network connections, and modified files, which is received from individual computers belonging to the corporate IT infrastructure and running the Microsoft Windows operating system.

Kaspersky Anti Targeted Attack Platform uses a table of alerts to display the detected signs of targeted attacks and intrusions into the corporate IT infrastructure.

The table of alerts does not display information on objects which satisfy at least one of the following conditions:

- The object has reputation *Trusted* in the KSN database.
- The object is digitally signed by a trusted vendor:
 - Kaspersky Lab.
 - Apple.
 - Google.

Information about these alerts is saved in the program database (on the Central Node or SCN).

Information about alerts in the database is rotated every night when the maximum allowed number of alerts is reached:

- Alerts generated by the **(IDS) Intrusion Detection System** and **(URL) URL Reputation** components have a maximum of 100000 alerts for each component.
- All other alerts have a maximum of 20000 alerts for each module or component.


If you are using distributed solution and multitenancy mode, rotation is performed on all SCNs and then synchronization with the PCN is performed. After synchronization, all deleted alerts are automatically deleted from the PCN.

The alerts table is in the **Alerts** section.




By default, this section displays information only on alerts that were not processed by users. To also display information on processed alerts, turn on the **Processed** switch in the upper-right corner of the window.

The table of alerts contains the following information:

1. **VIP** specifies if the alert has a status with special access rights. For example, alerts with the VIP status cannot be viewed by program users with the **Security officer** role.

2. **Created** is the time when the program generated the alert, and **Updated** is the time when the alert was updated.
3.  —Alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer or corporate LAN security based on Kaspersky Lab experience.

Alerts can have one of the following importance levels:

- **High**, marked with the  symbol—the alert has a high level of importance.
 - **Medium**, marked with the  symbol—the alert has a medium level of importance.
 - **Low**, marked with the  symbol—the alert has a low level of importance.
4. **Detected**—One or multiple categories of detected objects. For example, when the program detects a file infected with the Trojan-Downloader.JS.Cryptoload.ad virus, the **Detected**—Field shows Trojan-Downloader.JS.Cryptoload.ad for this alert.
 5. **Details**—Brief summary of the alert. For example: the name of a detected file or URL address of a malicious link.
 6. **Source**—Address of the source of the detected object. For example, this can be the email address from which a malicious file was sent, or the URL from which a malicious file was downloaded.
 7. **Destination**—Destination address of a detected object. For example, this can be the email address of your organization's mail domain to which a malicious file was sent, or the IP address of a computer on your corporate LAN to which a malicious file was downloaded.
 8. **Servers** is the list of names of servers which created the alert. Servers belong to the organization you are managing in the program web interface (see page [230](#)). Information about servers is displayed only when you are working in distributed solution and multitenancy mode.
 9. **Technologies**—Names of the program modules or components that generated the alert.

The **Technologies** column may indicate the following program modules and components:

- **(YARA) YARA.**
 - **(SB) Sandbox.**
 - **(URL) URL Reputation.**
 - **(IDS) Intrusion Detection System.**
 - **(AM) Anti-Malware Engine.**
 - **(TAA) Targeted Attack Analyzer.**
 - **(IOA) IOA Analysis.**
 - **(IOC) IOC Scanner.**
10. **State**—Alert status depending on whether or not this alert has been processed by the Kaspersky Anti Targeted Attack Platform user.

Alerts can have one of the following states:

- **New**—New alerts.
- **In process**—Alerts that a user of Kaspersky Anti Targeted Attack Platform is already processing.
- **Rescan**—Alerts resulting from a rescan of an object.

This column also displays the user name to which the alert was assigned. For example, Administrator.

If information in table columns is displayed as a link, you can click the link to open a list in which you can select the action to perform on the object. Depending on the type of value of the cell, you can perform one of the following actions:

- Any type of cell value:
 - **Filter by this value.**
 - **Exclude from filter.**
 - **Copy value to clipboard.**
- MD5 hash:
 - **Filter by this value.**
 - **Exclude from filter.**
 - **Find events.**
 - **Find on Kaspersky Threat Intelligence Portal.**
 - **Create a prevention rule.**
 - **Copy value to clipboard.**
- SHA256 hash:
 - **Filter by this value.**
 - **Exclude from filter.**
 - **Find events.**
 - **Find on Kaspersky Threat Intelligence Portal.**
 - **Create a prevention rule.**
 - **Copy value to clipboard.**

The **Intrusion Detection System** module consolidates information about processed network events in one alert when the following conditions are simultaneously met:

- The name of the triggered rule, version of program databases, and source all match for network events.
- No more than 24 hours elapsed between the events.

One alert is displayed for all network events that meet these conditions. The alert notification contains information only about the first network event.

Filtering and searching alerts

You can filter alerts to be displayed in the table of alerts for one or several columns of the table, or search for alerts in certain table columns according to the search criteria you specify.


You can create, save, and remove filters, and start filtering and searching alerts based on the conditions specified in saved filters.

If you are using distributed solution and multitenancy mode, you will not be able to save filters on the PCN.

Filters are saved for each user on the server on which they were created.

By default, this section displays information only on alerts that were not processed by users. To also display information on processed alerts, turn on the **Processed** switch in the upper-right corner of the window.

Filtering alerts by VIP status

You can filter alerts and search for alerts in the alerts table based on the  criterion, which indicates whether the alert has a status with special access rights. For example, alerts with the VIP status cannot be viewed by program users with the **Security officer** role.

► To filter alerts based on their VIP status:

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the heading of the **VIP** column to expand the list of filter settings.
3. Configure alert filtering settings:
 - If you want the table of alerts to display only alerts that have the VIP status, select **VIP**.
 - If you want the table of alerts to display all alerts, select **All**.

If neither is selected, the table shows all alerts.

The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by time

You can filter alerts and search the alert table by **Created** attribute, which is the time when the alert was created, as well as by **Updated** attribute, which is the time when the alert was updated.

► To filter or search alerts by time:


1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.

2. Click the **Created** link to open the list of alert display periods.
3. Select one of the following alert display periods from the **Time** list:
 - **All**, if you want the program to display all alerts in the table.
 - **Last hour**, if you want the program to display alerts that occurred during the last hour in the table.
 - **Last day**, if you want the program to display alerts that occurred during the last day in the table.
 - **Custom range**, if you want the program to display alerts that occurred during the period you specify in the table.
4. If you have selected the **Custom range** event display range, do the following:
 - a. In the calendar that opens, specify the start and end dates of the alert display period.
 - b. Click the **Apply** button.


The calendar closes.
5. If you want to filter alerts by update time, click **Switch time to Updated** in the upper part of the list and specify the period for which you want to display alerts.

The table of alerts displays only alerts matching the filter criteria you have set.

Filtering alerts by level of importance

You can filter events detected by the program as well as search the table of events for specific events based on the  **Importance** criterion, which indicates the alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer or corporate LAN security based on Kaspersky Lab experience.

► *To filter alerts based on their importance level:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click  to expand the filter settings list.
3. Select one or several of the following alert importance levels:
 - **High**—Alert has a high level of importance.
 - **Medium**—Alert has a medium level of importance.
 - **Low**—Alert has a low level of importance.

If no value is selected, the table shows alerts of all importance levels.


4. Click the **Apply** button.

The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by categories of objects detected

You can filter alerts and search the alerts table for specific alerts based on the **Detected** criterion, which indicates one or multiple categories of the object detected in the event. For example, if you want the table to display alerts about files infected by a specific virus, you can set a filter based on the name of this virus.

► *To filter or search alerts based on the category of detected objects:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the **Detected** link to open the filter configuration window.
3. In the drop-down list, select one of the following alert filtering operators:
 - **Contains.**
 - **Does not contain.**
4. In the entry field, type the name of a category (for example, Trojan) or several characters from the name of a category.
5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.


The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by obtained information

You can filter alerts and search the alerts table for specific alerts based on the **Details** criterion , which refers to brief information about the alert. For example: the name of a detected file or URL address of a malicious link.

► *To filter or search alerts based on obtained information:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the **Details** link to open the filter configuration window.
3. In the drop-down list on the left, select one of the following search criteria:
 - **Details.** The search will encompass all data on the detected object.
 - **ID.**
 - **File name.**
 - **File type.**
 - **MD5.**
 - **SHA256.**
 - **URL.**
 - **Domain.**
 - **User Agent.**
 - **Subject.**
 - **HTTP status.**
 - **Object source.**
 - **Object type.**

4. In the drop-down list on the right, select one of the following alert filtering operators:
 - **Contains.**
 - **Does not contain.**
 - **Equal to.**
 - **Not equal to.**
5. In the entry field, specify one or several characters of alert information.
6. To add a filter condition using a different criterion, click  and specify the filter condition.
7. Click the **Apply** button.


The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by source address

You can filter alerts and search the alerts table for specific alerts based on the **Source** criterion , which indicates the alert source address. For example, this can be the email address from which a malicious file was sent, or the IP address of the computer on your corporate LAN to which a malicious file was downloaded.

► *To filter or search alerts by source address:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the **Source** link to open the filter configuration window.
3. In the drop-down list, select one of the following alert filtering operators:
 - **Contains.**
 - **Does not contain.**
 - **Matches the pattern**
 - **Does not match the pattern**
4. In the entry field, specify one or several characters of the alert source address.


5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.

The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by destination address

You can filter alerts and search the alerts table for specific alerts based on the **Destination** criterion , which indicates the alert destination address. For example, this can be the email address of your organization's mail domain to which a malicious file was sent, or the IP address of a computer on your corporate LAN to which a malicious file was downloaded.

► *To filter or search alerts by destination address:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the **Destination** link to open the filter configuration window.
3. In the drop-down list, select one of the following alert filtering operators:
 - **Contains.**
 - **Does not contain.**
 - **Matches the pattern**
 - **Does not match the pattern**
4. In the text box, type one or more characters of the destination address of the detected objects.
5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.

The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by server name

You can filter alerts and search for alerts in the alerts table based on the **Servers** criterion, which indicates the name of servers that created the alert.

If you are using distributed solution and multitenancy mode, servers belong to the organization that you are managing in the program web interface (see page [230](#)). Filtering is available only on the PCN.

► *To filter or search alerts by server name:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click **Servers** to expand the list of servers which created alerts.
3. Select check boxes next to one or multiple server names.
4. Click the **Apply** button.

The table of alerts displays only alerts matching the filter criteria you have set.


Filtering and searching alerts based on names of program modules and components

You can filter alerts and search the alerts table for specific alerts based on the **Technologies** criterion, which indicates the names of program modules or components that generated the alert.

► *To filter alerts based on the names of program modules and components:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the **Technologies** link to open the filter configuration window.
3. In the drop-down list, select one of the following alert filtering operators:
 - **Contains**, if you want the program to display alerts generated by a program module or component that you specify.
 - **Does not contain**, if you want the program to hide alerts generated by a program module or component that you specify.
 - **Equal to**, if you want the program to display alerts generated by a program module or component that you specify.
 - **Not equal to**, if you want the program to hide alerts generated by a program module or component that you specify.
4. In the drop-down list on the right of the alert filtering operator that you have selected, select the name of the program module or component by which you want to filter alerts:
 - **(YARA) YARA.**
 - **(SB) Sandbox.**
 - **(URL) URL Reputation.**
 - **(IDS) Intrusion Detection System.**
 - **(AM) Anti-Malware Engine.**
 - **(TAA) Targeted Attack Analyzer.**
 - **(IOA) IOA Analysis.**
 - **(IOC) IOC Scanner.**

For example, if you want the program to display alerts generated by the Sandbox component, select the **Contains** filtering operator and the name of the **(SB) Sandbox** component.

5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.

The table of alerts displays only alerts matching the filter criteria you have set.

Filtering and searching alerts by the status of their processing by the user

You can filter alerts and search for them in the table of alerts based on the **State** criterion—alert status depending on whether or not this alert has been processed by the Kaspersky Anti Targeted Attack Platform user.

► *To filter or search alerts based on the status of their processing by the Kaspersky Anti Targeted Attack Platform user:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. To include processed alerts in the filter, turn on the **Processed** switch in the upper right corner of the window.
3. Click the **State** link to open a list of possible alert options depending on the status of their processing by the Kaspersky Anti Targeted Attack Platform user.
4. Select one of the following values:
 - **New**, if you want the program to display new alerts that no user has started to process.
 - **In process**, if you want the program to display alerts that a user of Kaspersky Anti Targeted Attack Platform is already processing.
 - **Rescan**, if you want the program to display alerts that resulted from a rescan.
5. In the **User name** field, specify a user name if you want to find alerts that have been assigned to a specific user with the **Senior security officer** or **Security officer** role.
6. Click the **Apply** button.

The table of alerts displays only alerts matching the filter criteria you have set.

Quickly creating an alert filter

► *To quickly create an alert filter:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Do the following to quickly add filter conditions to the filter being created:
 - a. Position the mouse cursor on the link containing the table column value that you want to add as a filter condition.
 - b. Left-click it.
This opens a list of actions to perform on the value.
 - c. In the list that opens, select one of the following actions:
 - **Filter by this value**, if you want to include this value in the filter condition.
 - **Exclude from filter**, if you want to exclude the value from the filter condition.
3. If you want to add several filter conditions to the filter being created, perform the actions to quickly add each filter condition to the filter being created.


The table of alerts displays only alerts matching the filter criteria you have set.

Clearing an alert filter

► *To clear an alert filter based on one or multiple filter conditions:*

1. Select the **Alerts** section in the window of the program web interface.

The table of alerts opens.

2. Click the  button to the right of the header of the alerts table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of alerts displays only alerts matching the filter criteria you have set.

Viewing alerts

The web interface of Kaspersky Anti Targeted Attack Platform displays the following types of alerts to inform users:

- A file has been downloaded or an attempt was made to download a file to a corporate LAN computer. The program detected this file in mirrored traffic on the organization's local network or in ICAP data of HTTP and FTP traffic, as well as HTTPS traffic if the administrator has configured SSL certificate replacement on the proxy server.
- A file has been sent to the email address of a user on the corporate LAN. The program detected this file in copies of email messages received via the POP3 or SMTP protocol, or received from the virtual machine or server with Kaspersky Secure Mail Gateway if it is being used in your organization.
- A website link was opened on a corporate LAN computer. The program detected this website link in mirrored traffic on the organization's local network or in ICAP data of HTTP and FTP traffic, as well as HTTPS traffic if the administrator has configured SSL certificate replacement on the proxy server.
- Network activity has occurred in which the IP address or domain name of a corporate LAN computer was detected. The program detected this network activity in mirrored traffic on the organization's local network.
- Processes have been started on a corporate LAN computer. The program detected these processes using the Endpoint Sensors module installed on individual computers that belong to the corporate IT infrastructure and run the Microsoft Windows operating system.

If a file was detected, the following information may be displayed in the program web interface depending on which program modules or components generated the alert:

- General information about the alert and the detected file (for example, the IP address of the computer on which the file was detected, and the name of the detected file).
- Results of the virus scan of the file performed by AM Engine.
- Results of scanning the file for signs of intrusion into the corporate IT infrastructure, performed by the YARA module.
- Results of analysis of the file's behavior in Windows XP SP3, 64-bit Windows 7, and 64-bit Windows 10 operating systems, performed by the Sandbox component.
- Results of analysis of APK executable files in the cloud infrastructure using machine learning technology.

If a website link was detected, the following information may be displayed in the program web interface depending on which program modules or components generated the alert:

- General information about the alert and the detected website link (for example, the IP address of the computer on which the website link was detected, and the address of the website link).
- Results of the link scan performed by the URL Reputation module for detecting of signs of malware, phishing URL addresses and URL addresses previously used by hackers for targeted attacks on the corporate IT infrastructure.

If the program detects network activity of the IP address or domain name of a computer on a corporate LAN, the program web interface may display the following information:

- General information about the alert and the detected network activity.
- Results of computer network activity scanning performed by the Targeted Attack Analyzer module.
- Results of web traffic scanning for signs of intrusion into the corporate IT infrastructure according to preset rules, performed by the Intrusion Detection System module (IDS).

If the program detects processes running on a corporate LAN computer where the Endpoint Sensors component is installed, the program web interface may display the following information:



- General information about the alert and processes running on the computer.
- Results of computer network activity scanning performed by the Targeted Attack Analyzer module.

Viewing information about an alert

► *To view information about an alert:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the line containing the alert whose information you want to view.
This opens a window containing information about the alert.

General information about an alert

The header of the window containing the alert information displays the alert ID. The  or  icon will be displayed next to the status depending on whether the alert has VIP status.

In the upper right corner of the window, alert status is displayed, depending on whether or not this alert has been processed by the Kaspersky Anti Targeted Attack Platform user.

The upper part of the window containing alert information may display the following general information about the alert:

- **Importance**—Alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer or corporate LAN security based on Kaspersky Lab experience.
- **Server** is the name of the server where the alert was generated. Servers belong to the organization you are managing in the program web interface (see page [230](#)).
- **Host**—Domain name of the computer where the alert occurred
- **Data source**—Source of the data. For example, SMTP Sensor or SPAN Sensor.
- **Time created**—Time when the alert was generated.
- **Time updated**—Time when information about the alert was updated.

Information in the Object information section

The **Object information** section can display the following event information about the detected file:

- **Object**—Name of the file.

By clicking the **Download** link next to the file name, you can download the file to the hard drive of your computer.

The file is downloaded in the form of a ZIP archive encrypted with the password “infected”. The name of the file inside the archive is replaced by the file's MD5 hash. The file extension of file inside the archive is not displayed.

- **Object type**—Type of the file. For example: ExecutableWin32.
- **File size**—Size of the file.
- **MD5**—MD5 hash of a file.

Clicking the link with **MD5** opens a list in which you can select one of the following actions:



- **Find on Kaspersky Threat Intelligence Portal.**
- **Find events.**
- **Create a prevention rule.**
- **Copy value to clipboard.**
- **SHA256**—SHA256 hash of a file.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- **Find on Kaspersky Threat Intelligence Portal.**
- **Find on virustotal.com.**
- **Find events.**
- **Create a prevention rule.**
- **Copy value to clipboard.**
- **Email from**—Email address from which the message containing the file was sent.
- **Email recipients**—One or more email addresses to which the message containing the file was sent.
- **Email subject**—Message subject.
- **Email headers**—Extended set of email message headers. For example, it can contain information about email addresses of the message sender and recipients, about mail servers that relayed the message, and the type of content in the email message.
- **File signed by**—File signature, if signed.

Information in the Alert information section

The **Alert details** section can display the following information about an alert:

-  or  —Alert importance for the Kaspersky Anti Targeted Attack Platform user depending on the impact this alert may have on computer or corporate LAN security based on Kaspersky Lab experience.
- **Time**—Time when the program generated the alert.
- **Detected**—One or multiple categories of detected objects. For example, when the program detects a file infected with the Trojan-Downloader.JS.Cryptoload.ad virus, the **Detected**—Field shows Trojan-Downloader.JS.Cryptoload.ad for this alert.
- **Method**—HTTP request method. For example, Get or Post.
- **URL**—Detected URL. It may also contain a response code.

Clicking the link with **URL** opens a list in which you can select one of the following actions:

- **Find on Kaspersky Threat Intelligence Portal.**
- **Find events.**

- **Copy value to clipboard.**
- **Referrer**—URL from which the user was redirected to the website link requiring attention. In the HTTP protocol, it is one of the headers in the client's request containing the request source URL.
- **Destination IP**—IP address of the resource requested by the user or the program.

Clicking the link with **Destination IP** opens a list in which you can select one of the following actions:

- **Find on Kaspersky Threat Intelligence Portal.**
- **Find events.**
- **Copy value to clipboard.**
- **User name**—Name of the user account whose actions led to the event.
- **Request/Response**—Length of the request and response.

Information in the Scan results section

The **Scan results** section can display the following results of alert scanning:

- The names of the program modules or components that generated the alert.
- One or multiple categories of the detected object. For example, the name of the virus can be shown: Virus.Win32.Chiton.i.
- Versions of databases of Kaspersky Anti Targeted Attack Platform modules and components that generated the alert.
- Results of alert scanning by program modules and components:

- **Anti-Malware Engine**—Category of the detected object based on the anti-virus database. For example, the name of the virus can be shown: Virus.Win32.Chiton.i.
- **Sandbox**—Results of a file behavior analysis performed by the Sandbox component.

You can view a detailed log of file behavior analysis in all operating systems by clicking the **Download debug info** link.

The file is downloaded in the form of a ZIP archive encrypted with the password “infected”. The name of the scanned file inside the archive is replaced by the file's MD5 hash. The file extension of file inside the archive is not displayed.

By default, the maximum hard drive space for storing file behavior scan logs is 300 GB in all operating systems. Upon reaching this limit, the program deletes the oldest file behavior scan logs and replaces them with new logs.

- **YARA**—Category of the detected file in YARA rules (for example, the category name susp_fake_Microsoft_signer may be displayed).
- **Intrusion Detection System**—Category of the detected object based on the Intrusion Detection System database. For example, the category Bot.AridViper.UDP.C&C might be displayed.
- **Targeted Attack Analyzer**—Information about the results of file analysis using Targeted Attack Analyzer technology.
- Name of the IOC file used to find the alert.

When selecting an IOC file, a window containing information about the alert is opened. The **IOC** section provides the XML code of the IOC file. The criterion by which the alert was generated is highlighted in yellow.

- Name of the IOA rule used to find the alert.

Clicking the link displays information about the IOA rule. If the IOA rule was provided by Kaspersky Lab experts, it contains information about the MITRE technique corresponding to the alert, as well as recommendations for reacting to the event.

- File size.
- MD5 hash of the file.
- Date and time when the alert was processed.

Information in the Network event section

You can click the **Download IDS artifact** link to download a file containing data about an alert.

The **Network event** section can show the following information about the link to the website opened on the computer:

- **Method**—Type of HTTP request, for example, GET or POST.
- **Source IP**—IP address of the computer on which the website link was opened.
- **Destination**—IP address of the computer on which the website link was opened.
- **User Agent**—Information about the browser that was used to download the file or to attempt to download the file, or to open the website link. It is the text string included in the HTTP request, which normally contains the name and version of the browser as well as the name and version of the operating system installed on the user's computer.

Information in the Sandbox scan results section

The **Sandbox scan results** section may display the following information about an alert:

- **File**—Full name and path of the scanned file.
- **File size**—Size of the file.
- **MD5**—MD5 hash of a file.

Clicking the link with **MD5** opens a list in which you can select one of the following actions:

- **Find on Kaspersky Threat Intelligence Portal.**
- **Find events.**
- **Create a prevention rule.**
- **Copy value to clipboard.**
- **Signed by**—Author of the certificate containing the digital signature for the detected file.
- **Detected**—One or multiple categories of detected objects. For example, when the program detects a file infected with the Trojan-Downloader.JS.Cryptoload.ad virus, the **Detected**—Field shows Trojan-Downloader.JS.Cryptoload.ad for this alert.

- **Time processed**—Time when the file was scanned.
- **Database versions**—Versions of the databases of modules and components of Kaspersky Anti Targeted Attack Platform that generated the alert.

Information about the file behavior analysis results is provided for each operating system in which the Sandbox component performed a scan. For the Windows 7 operating system (64-bit), you can view file activity logs for two Sandbox component scan modes: **Quick scan mode** and **Full logging mode**.

The following activity logs may be available for each scan mode:

- **Activity list**—Actions of the file within the operating system.
- **Activity tree**—Graphical representation of the file analysis process.
- **HTTP activity log**—Log of the file's HTTP activity. It contains the following information:
 - **Destination IP**—IP address to which the file is attempting to go from the operating system.
 - **Method**—HTTP request method, for example, GET or POST.
 - **URL**—URL of the website link that the file is attempting to open from the operating system.

Clicking the **Destination IP** and **URL** links opens a list in which you can select one of the following actions:

- **Find on Kaspersky Threat Intelligence Portal.**
 - **Find events.**
 - **Copy value to clipboard.**
- **IDS activity log**—Log of IDS actions. It contains the following information:
 - **Source IP**—IP address of the host on which the file is saved.
 - **Destination IP**—IP address to which the file is attempting to go from the operating system.
 - **Method**—HTTP request method, for example, GET or POST.
 - **URL**—URL of the website link that the file is attempting to open from the operating system.
- **DNS activity log**—Log of the file's DNS activity. It contains the following information:
 - **Request**—Name and type of the DNS-request.
 - **Response**—Name and type of the response from the DNS server, as well as the host name or the IP address of the computer from which this response was received.
- **Download full log** —Log of file behavior analysis in each operating system.

Information in the Remote hosts section

The **Remote hosts** section displays the list of hosts associated with the detected network activity. Click the link with name of a host to expand a block of information about the network activity associated with that host.

The following information is displayed:

- **Host name**—IP address or domain name of the computer with which the corporate LAN computer communicated.
- **Registrar** —Name of the domain registrar that registered this domain.
- **Domain info** —Detailed information on the domain.

- **Global popularity** —Popularity of the domain throughout the world.
- **Found on the local network** —Date and time when the host was detected by Kaspersky Anti Targeted Attack Platform.
- **Domain activity** —Information about domain activity is available if the alert was generated using data from the Endpoint Sensors component. The following information is displayed:
 - **Time** —Time when the activity was completed.
 - **Details** —Description of the completed operations.
 - **User name** —User account used to complete the activity.

Information in the Hosts section

The **Hosts** section displays the following information about hosts on which the IOA rule was triggered:

- **Host name**—IP address or domain name of the computer where the event occurred. Clicking the link opens the **Threat Hunting** section with the search condition containing the ID of the selected IOA rule and the selected host.
- **Number of events**—Number of events that occurred on the host.
- **Find events**. Clicking the link opens the **Threat Hunting** section with the search condition containing the ID of the selected IOA rule.

Information about network activity of the computer in the Processes section

The **Processes** section displays the list of processes associated with the detected network activity. By clicking the link with the path to the process, you can open the section of information about this process.

The following information is displayed:

- **File path**—Path to the process file.
- **Program name**—Name of the program that started the process.
- **File description**—Additional information about the detected file.
- **File size**—Size of the detected file.
- **File version**—Version of the detected file.
- **MD5**—MD5 hash of a file.
- **SHA256**—SHA256 hash of a file.
- **Vendor**—Company that released the program related to the process.
- **Program version**—Program version.
- **Signed by**—Author of the certificate containing the digital signature for the detected file.
- **Signature is valid**—Information on whether the digital signature is valid.
- **Found on the local network**—Date and time when the process was detected in the local network.
- **Found on computers**—Number of computers on which this process was detected in the local network.

- **Computers with similar activity**—Number of computers on which a similar process was detected.
- **Global file popularity**—Global popularity of the file that started the process.
- **Global path popularity**—Global popularity of the path by which the process was loaded.

You can click the **Process activity** link to open the section containing information about the network activity of a process:

- **Time**—Time of the network event.
- **Details**—Path to the process.
- **User name**—Name of the user account that started the process.

Information in the User account details section

The **User account details** section displays information about the user account of the computer on which the network activity was detected.

The following information is displayed:

- **Account type**—Type of account. For example, Administrator.
- **Login type**—Type of login to the computer.
- **Found on the network**—Date and time when the network activity was first detected in the local network.
- **Found on the computer**—Date and time when the activity was first detected on the computer.
- **Used on computers**—Number of computers on which similar network activity was detected.

Information in the Modules loaded into the process section

The **Modules loaded into the process** section displays information about the modules loaded into the process associated with the detected network activity. For example, a DLL library may be loaded into a process. By clicking the link with the path to the module, you can open the section of information about this process.

The following information is displayed:

- **File path**—Path to the file loaded into the process.
- **Program name**—Name of the file loaded into the process.
- **File description**—Additional information about the detected file.
- **File size**—Size of the detected file.
- **File version**—Version of the detected file.
- **MD5**—MD5 hash of a file.
- **SHA256**—SHA256 hash of a file.
- **Vendor**—Company that released the program related to the process.
- **Program version**—Program version.
- **Signed by**—Author of the certificate containing the digital signature for the detected file.

- **Signature is valid**—Information on whether the certificate is valid.
- **Found on the local network**—Date and time when the process was detected in the local network.
- **Found on computers**—Number of times this process was detected in the local network.
- **Computers with similar activity**—Number of computers on which a similar process was detected.
- **Global file popularity**—Global popularity of the file that started the process.
- **Global path popularity**—Global popularity of the path by which the process was loaded.

You can click the **View log** link to expand the section containing information about operations performed with the loaded module:

- **Time**—Time when the module was loaded.
- **Details**—Path to the loaded file.
- **User name**—Name of the user account that loaded the module.

Information in the Change log section

The **Change log** section can display the following alert information:

- Date and time of alert modification.
- Author of modifications.
For example, **System** or the program user name.
- Modification that occurred with the alert.

For example, an alert may be assigned to a VIP group, or it may be marked as processed.

Sending alert data

You can provide Kaspersky Lab with data about an alert (except the URL Reputation IOA Analysis, and IOC Scanner technologies) for further analysis.

To do so, you must copy the alert data to the clipboard and then email it to Kaspersky Lab.

Alert data may contain information about your organization that you consider to be confidential. You must consult with the security department of your organization for approval to send this data to Kaspersky Lab for further analysis.

► *To copy alert data to the clipboard:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the line containing the alert whose information you want to view.
This opens a window containing information about the alert.

3. Click the **Provide the alert details to Kaspersky Lab** link in the lower part of the window containing alert information.

The **Details** window opens.

4. View the alert data to be sent to Kaspersky Lab.
5. If you want to copy this data, click the **Copy to clipboard** button.

The alert data will be copied to the clipboard. You will be able to send it to Kaspersky Lab for further analysis.

User actions performed on alerts

When working in the program web interface under an account with the **Senior security officer** or **Security officer** role, you can perform the following actions on alerts:

- Assign an alert to themselves or to another user of the program web interface.
You can view all alerts assigned to a specific user by filtering alerts based on the status of their processing by the user(see page [244](#)).
- Mark an alert as processed.
You can view all alerts that have been processed by a specific user by filtering alerts based on the status of their processing by the user (see page [244](#)).
- Add a comment to an alert.
You can find commented alerts based on keywords within comments by filtering alerts based on received information (see page [241](#)).
- Mark the alert as VIP.
This action is available only to users with the **Senior security officer** role. Users with this role can view all alerts with the VIP status by filtering alerts by VIP status (see page [239](#)).

Assigning several alerts to a specific user

► *To assign an alert to yourself or to another user of the program web interface:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Select the check boxes opposite those alerts that you want to assign to a user.
You can select all alerts by selecting the check box in the table header.
3. In the pane that appears in the lower part of the window, click the arrow to the right of the **Mark as processed** button to expand the user list.
4. Select the user to whom you want to assign the alerts.
The action confirmation window opens.
5. Click the **Proceed** button.
The alerts will be assigned to the selected user.

You can view all alerts assigned to a specific user by filtering alerts based on the status of their processing by the user(see page [244](#)).

Assigning alerts to yourself or to another user

► *To assign one or multiple alerts to yourself or to another user:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.

2. Select the check boxes next to those alerts that you want to assign to yourself or to another user.

You can select all alerts by selecting the check box in the table header.

3. In the pane that appears in the lower part of the window, click the **Mark as processed** button.
4. The action confirmation window opens.

You can also leave a comment that will be displayed in the alert change history.

5. Click the **Proceed** button.

The alert will be assigned to the selected user.

You can view all alerts assigned to a specific user by filtering alerts based on the status of their processing by the user.

Marking the completion of single alert processing

► *To mark one alert assigned to you as processed in the alerts table:*

1. Select the **Alerts** section in the window of the program web interface.

The table of alerts opens.

2. In the **State** column of the alert that you want to mark as processed, click on your user name.
3. In the action list, select **Mark as processed**.

The alert will be marked as processed.

► *To mark an alert as processed in the course of managing that alert:*

1. Select the **Alerts** section in the window of the program web interface.

The table of alerts opens.

2. Open the alert that you want to mark as processed.
3. In the upper right corner of the window, click the arrow next to the button with the alert status to expand the list of actions.
4. In the action list, select **Mark as processed**.

The alert will be marked as processed. If the alert was assigned to a different user, it will be marked as processed by you.

You can view all alerts that have been processed by a specific user by filtering alerts based on the status of their processing by the user.

Marking the completion of alerts processing

► *To mark one or multiple alerts as processed:*

1. Select the **Alerts** section in the window of the program web interface.

The table of alerts opens.

2. Select the check boxes opposite those alerts that you want to mark as processed.

You can select all alerts by selecting the check box in the table header.

3. In the pane that appears in the lower part of the window, click the **Mark as processed** button.

The action confirmation window opens.

You can also leave a comment that will be displayed in the alert change history.

4. Click the **Proceed** button.

The selected alerts will be marked as processed. If the alerts were assigned to other users, they will be marked as processed by you.

You can view all processed alerts by filtering alerts based on the status of their processing by the user (see page [244](#)).

Modifying the status of VIP alerts

Users with the **Senior security officer** role can assign the VIP status to alerts or clear the VIP status of alerts.

► *To change the VIP status of alerts:*

1. Select the **Alerts** section in the window of the program web interface.

The table of alerts opens.

2. Select the check boxes next to those alerts whose VIP status you want to change.

You can select all alerts by selecting the check box in the table header.

3. Do one of the following:

- If you want to mark alerts as VIP, click the **Mark as VIP** button in the pane that appears in the lower part of the window.
- If you want to remove the VIP status from alerts, select **Mark as non-VIP** in the **Mark as VIP** drop-down list in the pane that appears in the lower part of the window.

The action confirmation window opens.

You can also leave a comment that will be displayed in the alert change history.

4. Click the **Proceed** button.

The VIP status of alerts is changed.

Users with the **Senior security officer** role can view all events with the VIP status by filtering alerts by VIP status (see page [239](#)).

Adding a comment to an alert

► *To add a comment to an alert:*

1. Select the **Alerts** section in the window of the program web interface.

The table of alerts opens.

2. Select an alert for which you want to add a comment.

This opens a window containing information about the alert.

3. In the comment entry field under the name of the **Change log** section, enter a comment for the alert.

4. Click the **Add** button.

The comment will be added to the alert and will be displayed in the **Change log** section of this alert.

You can find commented alerts based on keywords within comments by filtering alerts based on received information (see page [241](#)).

Events database threat hunting

When working in the program web interface, users with the **Senior security officer** or **Security officer** roles can generate search queries and use IOC files and IOA rules to search the events database for threats, for organizations whose data they are allowed to access (see page [160](#)).

To form search queries through the events database, you can use *design mode* or *source code mode*.

In design mode, you can create and modify search queries using drop-down lists with options for the type of field value and operators.

In source code mode (see page [262](#)), you can create and modify search queries using text commands.

You can upload an IOC file (see page [264](#)) and search for events based on conditions defined in this IOC file.

You can also create IOA rules (see page [265](#)) based on event search conditions.

Searching events using design mode

► *To define event search conditions in design mode:*

1. In the program web interface window, select the **Threat Hunting** section, **Builder** or **Source code** tab.
The event search form opens.
2. In the drop-down list, select the criterion for searching for events in one of the following groups:
 - **Full text search.**
 - **General details.**
 - **IOA properties.**
 - **File properties.**
 - **Process started.**
 - **Remote connection.**
 - **Registry modified.**
 - **Windows Log event.**
 - **Host name changed.**
 - **Detect and processing result.**
3. In the drop-down list, select one of the following comparison operators:
 - **=**
 - **!=**
 - **CONTAINS**
 - **!CONTAINS**
 - **STARTS**
 - **!STARTS**
 - **ENDS**

- **!ENDS**

- **>**

- **<**

Each type of value of the field has its own relevant set of comparison operators. For example, when the **EventType** field value type is selected, the **=** and **!=** operators will be available.

- Depending on the selected type of field value, perform one of the following actions:
 - In the field, specify one or several characters by which you want to perform an event search.
 - In the drop-down list, select the field value option by which you want to perform an event search.

For example, to search for a full match based on a user name, enter the user name.
- If you want to add a new condition, use the **AND** or **OR** logical operator and repeat the necessary actions for adding a condition.
- If you want to add a group of conditions, click the **Group** button and repeat the actions necessary for adding conditions.
- If you want to delete a group of conditions, click the **Remove group** button.
- If you want to search events that occurred during a specific period, in the **Any time** drop-down list select one of the following event search periods:
 - Any time**, if you want the table to display events found for any period of time.
 - Last hour**, if you want the table to display events that were found during the last hour.
 - Last day**, if you want the table to display events found during the last day.
 - Custom range**, if you want the table to display events found during the period you specify.
- If you have selected the **Custom range** display period for found events:
 - In the calendar that opens, specify the start and end dates of the event display range.
 - Click the **Apply** button.

The calendar closes.

- Click the **Search** button.

Grouping levels of found events are displayed: **All hosts** – Organization names – Server names.

- Click the name of the server for which you want to view events.

The host table of the selected server opens. Event grouping levels are displayed above the table. The host table contains the following information:

- Host** is the name of the host on which the event was detected.
- Number of events** is the number of events that were detected on the host.
- First event** is the detection date and time of the first event on this host.
- All hosts** is the detection date and time of the latest event on this host.

- Select the host for which you want to view events.

This opens a table of events matching the search conditions you specified. Event grouping levels are displayed above the table.

You can return to the host selection window by clicking the link with the organization name and the server name, or return to organization and server selection by clicking the **All hosts** link.

Searching events using source code mode

► *To define event search conditions in source code mode:*

1. Select the **Threat Hunting** section, **Source code** tab in the program web interface window.
This opens a form containing the field for entering event search conditions in source code mode.
2. Enter the event search conditions using commands, the logical operators **OR** and **AND**, and parentheses for creating groups of conditions.
Commands must match the following syntax: `<field type> <comparison operator> <field value>`.

Example:

```
EventType = "filechange"
AND (
    FileName CONTAINS "example"
    OR UserName = "example"
)
```

3. If you want to search events that occurred during a specific period, click the **Any time** button and select one of the following event search periods:
 - **Any time**, if you want the table to display events found for any period of time.
 - **Last hour**, if you want the table to display events that were found during the last hour.
 - **Last day**, if you want the table to display events found during the last day.
 - **Custom range**, if you want the table to display events found during the period you specify.
4. If you have selected the **Custom range** display period for found events:
 - a. In the calendar that opens, specify the start and end dates of the event display range.
 - b. Click the **Apply** button.
The calendar closes.
5. Click the **Search** button.
Grouping levels of found events are displayed: **All hosts** – Organization names – Server names.
6. Click the name of the server for which you want to view events.
The host table of the selected server opens. Event grouping levels are displayed above the table. The host table contains the following information:

- **Host** is the name of the host on which the event was detected.
 - **Number of events** is the number of events that were detected on the host.
 - **First event** is the detection date and time of the first event on this host.
 - **All hosts** is the detection date and time of the latest event on this host.
7. Select the host for which you want to view events.
- This opens a table of events matching the search conditions you specified. Event grouping levels are displayed above the table.

You can return to the host selection window by clicking the link with the organization name and the server name, or return to organization and server selection by clicking the **All hosts** link.

Changing the event search conditions

► *To change the event search conditions, perform the following actions in the **Threat Hunting** section of the program web interface window:*

1. Click the form containing the event search conditions in the upper part of the window.
2. Select one of the following tabs:
 - **Builder**, if you want to change the event search conditions in design mode.
 - **Source code**, if you want to change the event search conditions in source code mode.
3. Make the relevant changes.
4. Click one of the following buttons:
 - **Refresh**, if you want to refresh the current event search with the new conditions.
 - **New search**, if you want to perform a new event search.

Grouping levels of found events are displayed: **All hosts** – Organization names – Server names.

5. Click the name of the server for which you want to view events.
- The host table of the selected server opens. Event grouping levels are displayed above the table. The host table contains the following information:
- **Host** is the name of the host on which the event was detected.
 - **Number of events** is the number of events that were detected on the host.
 - **First event** is the detection date and time of the first event on this host.
 - **All hosts** is the detection date and time of the latest event on this host.
6. Select the host for which you want to view events.
- This opens a table of events matching the search conditions you specified. Event grouping levels are displayed above the table.

You can return to the host selection window by clicking the link with the organization name and the server name, or return to organization and server selection by clicking the **All hosts** link.

Uploading an IOC file and searching for events based on conditions defined in the IOC file

► *To upload an IOC file and search for events based on conditions defined in the IOC file:*

1. Select the **Threat Hunting** section in the program web interface window.

The event search form opens.

2. Click the **Upload** button.

The file selection window opens.

3. Select the IOC file that you want to upload and click the **Open** button.

The IOC file will be uploaded.

On the **Source code** tab, the form containing event search conditions will display the conditions defined in the uploaded IOC file.

You can search for events that match these conditions. You can also change the conditions defined in an uploaded IOC file, or add event search conditions in source code mode (see page [262](#)).

4. If you want to search events that occurred during a specific period, click the **Any time** button and select one of the following event search periods:

- **Any time**, if you want the table to display events found for any period of time.
- **Last hour**, if you want the table to display events that were found during the last hour.
- **Last day**, if you want the table to display events found during the last day.
- **Custom range**, if you want the table to display events found during the period you specify.

5. If you have selected the **Custom range** display period for found events:

- a. In the calendar that opens, specify the start and end dates of the event display range.
- b. Click the **Apply** button.

The calendar closes.

6. Click the **Search** button.

Grouping levels of found events are displayed: **All hosts** – Organization names – Server names.

7. Click the name of the server for which you want to view events.

The host table of the selected server opens. Event grouping levels are displayed above the table. The host table contains the following information:

- **Host** is the name of the host on which the event was detected.
- **Number of events** is the number of events that were detected on the host.
- **First event** is the detection date and time of the first event on this host.

- **All hosts** is the detection date and time of the latest event on this host.
8. Select the host for which you want to view events.

This opens a table of events matching the search conditions you specified. Event grouping levels are displayed above the table.

You can return to the host selection window by clicking the link with the organization name and the server name, or return to organization and server selection by clicking the **All hosts** link.

Creating an IOA rule based on event search conditions

► *To create an IOA rule based on event search conditions:*

1. Select the **Threat Hunting** section in the program web interface window.

The event search form opens.

2. Perform an event search using design mode or source code mode.
3. Click the **Save as IOA rule** button.

The **Save** window opens.

4. In the **New IOA rule name** field, enter the name of the IOA rule.
5. Click the **Save** button.

The event search condition will be saved. The new IOA rule with the specified name is displayed in the **IOC/IOA Analysis** section, **IOA Analysis** subsection.

Event information

When working in the program web interface, **Senior security officer** and **Security officer** users can view event information for organizations to which they have access (see page [160](#)).

If you are using the distributed solution and multitenancy mode, the section displays data on the organization that you chose (see page [230](#)).

► *To enable the display of events for all organizations:*

Turn on the **Search on all companies** toggle switch.

Viewing the table of events

The events table is displayed in the **Threat Hunting** section of the program web interface window after completion of the search for threats in the events database (see page [260](#)).

Events are grouped by hosts of the selected servers and organizations. The table of events contains the following information:

1. **Event time**—Date and time when the event was detected.
2. **Event**—Type of event.
3. **Details**—Information about the event.
4. **User name**—Name of the user.

Each type of event has its own type of cell value in the **Details** column of the events table (see the table below).

Table 13. Correspondence of the types of cell values in the **Event** and **Details** columns

Event	Details
Process started	Name of the process file that was started. SHA256- and MD5 hash.
Module loaded	Name of the dynamic library that was loaded. SHA256- and MD5 hash.
Remote connection	URL to which a remote connection attempt was made. Name of the file that attempted to establish a remote connection.
Prevention rule	Name of the file of the application that was blocked from starting. SHA256- and MD5 hash.
Document blocked	Name of the document that was blocked from starting. SHA256- and MD5 hash.
File created	Name of the created file. SHA256- and MD5 hash.
Windows Log event	Windows event logging channel. Event type ID.

Event	Details
Registry modified	Name of key in registry. <name of the variable in the key>=<value of the variable>.
Port listened	Server address and port. Name of the file of the process that listens to the port.
Driver loaded	File name of the driver that has been loaded. SHA256- and MD5 hash.
Host name changed	Old host name. New host name.

Clicking the link with the name of the event type, data, additional information and user name opens a list in which you can select the action to perform on the object. Depending on the type of value of the cell, you can perform one of the following actions:

- Any type of cell value:
 - Filter by this value.**
 - Exclude from filter.**
 - Copy value to clipboard.**
- File name:
 - Kill process.**
 - Delete file.**
 - Get file.**
 - Quarantine file.**
- MD5 hash:
 - Find on Kaspersky Threat Intelligence Portal.**
 - Create a prevention rule.**
 - Find in Storage.**
- SHA256 hash:
 - Find on Kaspersky Threat Intelligence Portal.**
 - Find on virustotal.com.**
 - Create a prevention rule.**
 - Find in Storage.**

Viewing information about an event

► *To view information about an event:*

- In the program web interface window, select the **Threat Hunting** section, **Builder** or **Source code** tab.
The event search form opens.
- If you are using distributed solution and multitenancy mode and want to enable the display of events for all organizations, turn on the **Search on all companies** toggle switch.

3. Perform an event search using design mode (see page [260](#)) or source code mode (see page [262](#)).

Grouping levels of found events are displayed: **All hosts** – Organization names – Server names.

4. Click the name of the server for which you want to view events.

The host table of the selected server opens. Event grouping levels are displayed above the table. The host table contains the following information:

- **Host** is the name of the host on which the event was detected.
- **Number of events** is the number of events that were detected on the host.
- **First event** is the detection date and time of the first event on this host.
- **All hosts** is the detection date and time of the latest event on this host.

5. Select the host for which you want to view events.

This opens a table of events matching the search conditions you specified. Event grouping levels are displayed above the table.

You can return to the host selection window by clicking the link with the organization name and the server name, or return to organization and server selection by clicking the **All hosts** link.

6. Select the event whose information you want to view.

This opens a window containing information about the event.

Information about process startup

The window showing information about **Process started** events contains the following details:

- Tree of events.

Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.

You can select events in the tree of events to view information about these events.

- **Process started:**

- **Event time**—Process start time.
- **File**—Process file name.
- **Launch parameters**—Process startup settings.
- **MD5**—MD5 hash of the process file.
- **SHA256**—SHA256 hash of the process file.
- **Size**—Size of the process file.
- **Process ID**—Process identifier.
- **Process end time**—Time when the process was terminated.
- **Time created**—Process file creation time.
- **Time modified**—Time of last modification of the process file.

- **Host name**—Name of the host on which the process was started.
- **User name**—Name of the user that started the process.
- **Parent process:**
 - **File**—Path to the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.
 - **Process ID**—Identifier of the parent process.

Information about module loading

The window showing information about **Module loaded** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Module loaded:**
 - **Event time**—Time when the module was loaded.
 - **File**—Name of the loaded module file.
 - **MD5**—MD5 hash of the loaded module file.
 - **SHA256**—SHA256 hash of the loaded module file.
 - **Host name**—Name of the host on which the module was loaded.
 - **User name**—Name of the user that loaded the module.
 - **Size**—Size of the loaded module.
 - **Time created**—Creation time of the loaded module.
 - **Time modified**—Date of last modification of the loaded module.
- **Parent process:**
 - **File**—Name of the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.

Information about a remote connection

The window showing information about **Remote connection** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.

- **Remote connection:**
 - **Event time**—Time of the remote connection attempt.
 - **Remote IP**—IP address of the host to which a remote connection attempt was made.
 - **Local IP**—IP address of the local computer from which a remote connection attempt was made.
 - **Host name**—Host name from which a remote connection attempt was made.
 - **User name**—Name of the user that attempted to establish a remote connection.
- **Parent process:**
 - **File**—Name of the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.

Information about prevention rule triggering

The window showing information about **Prevention rule** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Prevention rule:**
 - **Event time**—Time when the file startup prevention was triggered.
 - **File**—Name of the file that was prevented from running.
 - **Launch parameters**—Parameters that were used for the attempt to run the file.
 - **MD5**—MD5 hash of the file that was prevented from running.
 - **SHA256**—SHA256 hash of the file that was prevented from running.
 - **Size**—Size of the file that was prevented from running.
 - **Time created**—Creation time of the file that was prevented from running.
 - **Time modified**—Date of last modification of the file that was prevented from running.
 - **Host name**—Name of the host on which the file startup prevention was triggered.
 - **User name**—Name of the user that attempted to run the file.
- **Parent process:**
 - **File**—Name of the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.
 - **Process ID**—Identifier of the parent process.

Information about document blocking

The window showing information about **Document blocked** events contains the following details:

- Tree of events.
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Document blocked:**
 - **Event time**—Time when the document was blocked.
 - **File**—Name of the blocked document.
 - **MD5**—MD5 hash of the blocked document.
 - **Process file** – name of the file of the process that attempted to open the document.
 - **Process MD5** – MD5 hash of the process that attempted to open the document.
 - **Process SHA256** – SHA256 hash of the process that attempted to open the document.
 - **Process ID**—Identifier of the process that attempted to open the document.
 - **Host name**—Name of the host on which the document was blocked.
 - **User name**—Name of the user that attempted to open the document.
- **Parent process:**
 - **File**—Name of the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.
 - **Process ID**—Identifier of the parent process.

Information about file creation

The window showing information about **File created** events contains the following details:

- Tree of events.
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **File created:**
 - **Event time**—Time when the event was detected.
 - **File**—Name of the created file.
 - **MD5**—MD5 hash of the created file.
 - **SHA256**—SHA256 hash of the created file.
 - **Size**—Size of the created file.
 - **Time created**—Time when the file was created.

- **Time modified**—Time of last modification of the file.
- **Host name**—Name of the host on which the file was created.
- **User name**—Name of the user that created the file.
- **Parent process:**
 - **File**—Path to the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.

Information about an event in the Windows log

The window showing information about **Windows Log event** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Windows Log event:**
 - **Event time**—Time when the event was detected.
 - **Security event ID**—Identifier of the type of security event in the Windows log.
 - **Record ID**—Event ID in the Windows log.
 - **Provider**—Name of the provider.
 - **Log name**—Name of the Windows log.
 - **Domain**—Domain of the host on which the event occurred.
 - **Host name**—Name of the host on which the event occurred.
 - **User name**—User name of the host on which the event occurred.

The **Windows Log event** settings group also contains data from the Windows system log. The scope of data depends on the type of Windows event.

Information about changes in the registry

The window showing information about **Registry modified** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Registry modified:**
 - **Event time**—Time of registry modification.
 - **Registry key path**—Path to the registry key in which the change was made.

- **Registry value name**—Name of the registry parameter.
- **Registry value**—Value of the registry parameter.
- **Host name**—Name of the host on which the registry modification was made.
- **User name**—Name of the user that made the change in the registry.
- **Parent process:**
 - **File**—Path to the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.

Information about port listening

The window showing information about **Port listened** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Port listened:**
 - **Event time**—Port listening time.
 - **Port**—Port that was listened to.
 - **Local IP**—IP address of the network interface whose port was listened to.
 - **Host name**—Name of the host whose port was listened to.
 - **User name**—Name of the user whose account was used to listen to the port.
- **Parent process:**
 - **File**—Path to the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.

Information about driver loading

The window showing information about **Driver loaded** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Driver loaded:**
 - **Event time**—Time when the driver was loaded.
 - **File**—Name of the loaded driver file.

- **MD5**—MD5 hash of the loaded driver file.
- **SHA256**—SHA256 hash of the loaded driver file.
- **Host name**—Name of the host on which the driver was loaded.
- **Size**—Size of the loaded driver.
- **Time created**—Creation time of the loaded driver.
- **Time modified**—Time of last modification of the loaded driver.

Information about changing a host name

The window showing information about **Host name changed** events contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- **Host name changed:**
 - **Event time**—Time when the host name was changed.
 - **Host name**—New host name.
 - **User name**—Name of the user that changed the host name.
 - **Old host name**—Old host name.

Information about the alert

The window showing information about a **Detect** type event contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- On the **Details** tab, under **Detect**:
 - **Event time**—Date and time of the event.
 - **Detected object**—Name of the detected object. To find all events in which the object was detected, click the name of the object, then click **Find events**.
 - **Last action**—Last action taken on the detected object.
 - **Host name**—Name of the host on which the alert was generated.
 - **User name**—User account used to complete the action taken on the detected object.
 - **Object type**—Type of object (for example, a file).
 - **Object name**—Full name of the file in which the object was detected.
 - **MD5**—MD5 hash of the file in which the object was detected.

- **SHA256**—SHA256 hash of the file in which the object was detected.
- **Detect mode**—Scan mode in which the alert was generated.
- **Record ID**—ID of the record of the alert in the database.
- **Databases version**—Version of the database used to generate the alert.
- On the **Details** tab, under **Parent process**:
 - **File**—Path to the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.
 - **Process ID**—Identifier of the parent process.
 - **Launch parameters**—Parent process startup settings.
- On the **History** tab, in the table:
 - **Type**—Type of the event: **Detect** and **Detect processing result**.
 - **Description**—Description of the event.
 - **Time**—Date and time of detection and alert processing result.

Information about alert processing results

The window showing information about a **Detect processing result** type event contains the following details:

- **Tree of events.**
Displays the parent events and child events, and the links between them. The root node of the tree of events is the host whose events you are viewing.
You can select events in the tree of events to view information about these events.
- On the **Details** tab, under **Detect processing result**:
 - **Event time**—Date and time of the event.
 - **Detected object**—Name of the detected object. To find all events in which the object was detected, click the name of the object, then click **Find events**.
 - **Last action**—Last action taken on the detected object.
 - **Host name**—Name of the host on which the alert was generated.
 - **User name**—User account used to complete the action taken on the detected object.
 - **Object type**—Type of object (for example, a file).
 - **Object name**—Full name of the file in which the object was detected.
 - **MD5**—MD5 hash of the file in which the object was detected.
 - **SHA256**—SHA256 hash of the file in which the object was detected.
 - **Detect mode**—Scan mode in which the alert was generated.
 - **Record ID**—ID of the record of the alert in the database.
 - **Databases version**—Version of the database used to generate the alert.

- On the **Details** tab, under **Parent process**:
 - **File**—Path to the parent process file.
 - **MD5**—MD5 hash of the parent process file.
 - **SHA256**—SHA256 hash of the parent process file.
 - **Process ID**—Identifier of the parent process.
 - **Launch parameters**—Parent process startup settings.
- On the **History** tab, in the table:
 - **Type** is the type of the **Detect processing result** event.
 - **Description**—Description of the event.
 - **Time** is the date and time of the alert processing result.

Managing the Endpoint Sensors component

The Endpoint Sensors component (see page [40](#)) is installed on separate computers (hereinafter referred to as “hosts”) that belong to the corporate IT infrastructure and run a Microsoft Windows operating system. Continuously monitors processes running on those computers, active network connections, and files that are modified.

Users with **Senior security officer**, **Security officer**, **Local administrator**, and **Administrator** roles can assess how regularly data is received from hosts on which the Endpoint Sensors component is installed, on the **Endpoint Sensors** tab of the program web interface window for organizations whose data the user is allowed to access (see page [160](#)). If you are using distributed solution and multitenancy mode, the web interface of the PCN server displays the list of Endpoint Sensors components for the PCN and all connected SCNs.

Users with the **Local administrator** and **Administrator** roles can configure the display of how regularly data is received from hosts with the Endpoint Sensors installed, for organizations whose data they are allowed to access (see page [160](#)).

If suspicious network activity is detected, users with the **Senior security officer** role can isolate (see page [291](#)) any host with the Endpoint Sensors component from the network, for organizations whose data the user is allowed to access (see page [160](#)). In this case, the connection between the server with the Central Node component and a host with the Endpoint Sensors component will not be interrupted.

For support in case of faulty operation of the Endpoint Sensors component, Technical Support experts may ask you to perform the following actions for debugging purposes (including in Technical Support Mode):

- Activate collection of extended diagnostic information.
- Modify the settings of individual program components.
- Modify the settings for storing and sending the obtained diagnostic information.
- Configure network traffic to be intercepted and saved to a file.

Technical Support experts will provide all the information needed to perform these operations (description of the sequence of steps, settings to be modified, configuration files, scripts, additional command line functionality, debugging modules, special-purpose utilities, etc.) and inform you about the scope of data gathered for debugging purposes. The extended diagnostic information that is gathered is saved on the user's computer. The collected data is not automatically sent to Kaspersky Lab.

The operations listed above should be performed only when instructed by and under the supervision of Technical Support experts. Unsupervised changes to program settings performed in ways other than those described in the Administrator's Guide or according to the instructions of Technical Support experts can slow down or crash the operating system, reduce computer security, or compromise the availability and integrity of data being processed.

Viewing the Endpoint Sensors table on a standalone Central Node server

The table of hosts with the Endpoint Sensors component is located in the **Endpoint Sensors** section of the program web interface window.

If you are using a standalone Central Node server, but not using KSC integration, distributed solution and

multitenancy mode, the host table with the Endpoint Sensors component can display the following data:

- **Host**—Host name with the Endpoint Sensors component.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Version**—Version of the Endpoint Sensors component installed.
- **Activity**—Activity indicator of the Endpoint Sensors component. Possible values:
 - **Normal activity** for hosts from which latest data was recently received.
 - **Warning** for hosts from which latest data was received a long time ago.
 - **Critical inactivity** for hosts from which latest data was received an extremely long time ago.

Clicking any column of the table opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

Viewing the Endpoint Sensors table on a standalone Central Node server with KSC integration

If you have configured integration with KSC, the table of hosts with the Endpoint Sensors component is located in the **Endpoint Sensors** section of the program web interface window.

The **Endpoint Sensors** section includes the following tabs:

- **Central Node**. Displays information about hosts with the Endpoint Sensors component that are connected to this Central Node server.
- **KSC**. Displays information about all hosts connected to KSC.

The **Central Node** tab can display the following information:

- **Host**—Host name with the Endpoint Sensors component.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Version**—Version of the Endpoint Sensors component installed.
- **Activity**—Activity indicator of the Endpoint Sensors component. Possible values:
 - **Normal activity** for hosts from which latest data was recently received.
 - **Warning** for hosts from which latest data was received a long time ago.
 - **Critical inactivity** for hosts from which latest data was received an extremely long time ago.

The **KSC** tab can display the following information:

- **Host**—Host name with the Endpoint Sensors component.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.

- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Endpoint Sensor**—Type of component used as an Endpoint Sensors component.

A component may be one of the following types:

- **Endpoint Sensor.**

The Endpoint Sensors component (see page [40](#)) that was installed from the Kaspersky Anti Targeted Attack Platform package.

- **Built-in KES.**

The Endpoint Sensors component that is included in Kaspersky Endpoint Security for Windows.

- **Version**— version of the Endpoint Sensors component installed.
- **Server**—Name of the server with the Central Node component.
- **Sensor state**—Status of the Endpoint Sensors component installed on the computer.

An Endpoint Sensors component can have one of the following statuses:

- **Running.**
- **Stopped.**
- **Failure.**
- **Not installed.**

- **Host state**—Host status of the computer with the Endpoint Sensors component.

A host can have one of the following states:

- **Offline**
- **Online**

- **Errors**—Error status in the operation of the Endpoint Sensors component. The status can take the value **No errors** or can contain information about the type of error in the operation of the Endpoint Sensors component.

Clicking any column of the table opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

By clicking the link with the IP address of the computer where the Endpoint Sensors component is installed, you can also choose the **Navigate to alerts filtered by this value** action.

Clicking the link with the name of the host on which the Endpoint Sensors is installed allows you to select the following actions:

- **Isolate from network.**
- **Find events.**
- **Find alerts.**

Viewing the Endpoint Sensors table in distributed solution and multitenancy mode

The table of hosts with the Endpoint Sensors component is located in the **Endpoint Sensors** section of the program web interface window.

If you are using the distributed solution and multitenancy mode, but are not using integration with KSC, the table contains information about the Endpoint Sensors components connected to the PCN and all SCN servers. The table can display the following data:

- **Host**—Host name with the Endpoint Sensors component.
Clicking the link with the host name opens a list in which you can select one of the following actions:
 - **Filter by this value.**
 - **Exclude from filter.**
 - **New prevention rule.**
 - **Find events.**
 - **Find alerts.**
 - **Copy value to clipboard.**
- **Servers**—Names of servers to which the host with the Endpoint Sensors is connected.
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Version**—Version of the Endpoint Sensors component installed.
- **Activity**—Activity indicator of the Endpoint Sensors component. Possible values:
 - **Normal activity** for hosts from which latest data was recently received.
 - **Warning** for hosts from which latest data was received a long time ago.
 - **Critical inactivity** for hosts from which latest data was received an extremely long time ago.

Clicking any column of the table opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

By clicking the link with the IP address of the computer where the Endpoint Sensors component is installed, you can also choose the **Navigate to alerts filtered by this value** action.

Viewing information about a host

► *To view information about a host:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
2. Select the host for which you want to view information.

This opens a window containing information about the host.

The window contains the following information:

- The **Alerts** link opens the **Alerts** section with the search condition containing information about your selected host.
- Clicking the **Events** link opens the **Threat Hunting** section with the search condition containing information about your selected host.
- **State**—Status of the host with the Endpoint Sensors component.

A host can have one of the following states:

- **Online**
- **Offline**
- **Host**—Host name with the Endpoint Sensors component.



You can click the link with the host name to select one of the following actions:

- **Kill process.**
- **Delete file.**
- **Get file.**
- **Quarantine file.**
- **Run program.**
- **New prevention rule.**
- **Isolate from network.**
- **Find events.**
- **Find alerts.**
- **Copy value to clipboard.**
- **IP**—IP address of the computer where the Endpoint Sensors component is installed.
- **OS**—Version of the operating system that is installed on the computer with the Endpoint Sensors component.
- **Protection**—Host status with the Endpoint Sensors component.
- **Server**—Name of the SCN or PCN server. Only displayed in distributed solution and multitenancy mode.
- **Server name**—Name of the Central Node server.
- **Last connection**—time of the last connection to the Central Node, SCN, or PCN server.
- **Version**—Type and version of the Endpoint Sensors component installed.
- **Status**—Status of the Endpoint Sensors component.
- **Preventions.** Clicking the link opens a table of prevention rules created from file hashes on this host, containing the following information:
 - **Type**
 - **Name.**
 - **State.**
 - **Hash.**

- **Tasks.** Clicking the link opens the table of tasks created for this host containing the following information:
 - **Time created.**
 - **Type.**
 - **Name.**
 - **Details.**
 - **State.**

Filtering and searching Endpoint Sensors by host name

► *To filter or search for hosts with the Endpoint Sensors component by host name:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Host** link to open the filter configuration window.
4. If you want to display only isolated hosts, select the **Show isolated Endpoint Sensors only** check box.
5. In the drop-down list, select one of the following filtering operators:
 - **Contains.**
 - **Does not contain.**
6. In the entry field, specify one or several characters of the host name.
7. To add a filter condition using a different criterion, click  and specify the filter condition.
8. If you want to delete the filter condition, click the  button to the right of the field.
9. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors that have been isolated from the network

- *To filter or search for hosts with the Endpoint Sensors component that are isolated from the network (see page [291](#)):*
1. Select the **Endpoint Sensors** section in the window of the program web interface.

This will open the table of hosts with the Endpoint Sensors component.

2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Host** link to open the filter configuration window.
4. Select the **Show isolated Endpoint Sensors only** check box.
5. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by PCN and SCN server names

If you are using distributed solution and multitenancy mode, you can filter or find hosts with the Endpoint Sensors component based on the names of PCN and SCN servers to which those hosts are connected.

- *To filter or search for hosts with the Endpoint Sensors component by the names of PCN and SCN servers:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. Click the **Servers** link to open the filter configuration window.
3. Select check boxes next to names of servers by which you want to filter or search for hosts with the Endpoint Sensors component.
4. Click the **Apply** button.



The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by computer IP address

- *To filter or search for hosts with the Endpoint Sensors component based on the IP address of the computer with the Endpoint Sensors component installed:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **IP** link to open the filter configuration window.
4. In the drop-down list, select one of the following filtering operators:
 - **Contains.**
 - **Does not contain.**
5. In the entry field, specify one or several characters of the computer IP address. You can enter the IP address or subnet mask in IPv4 format (for example, 192.0.0.1 or 192.0.0.0/16).
6. To add a filter condition using a different criterion, click  and specify the filter condition.
7. If you want to delete the filter condition, click the  button to the right of the field.
8. Click the **Apply** button.

The filter configuration window closes.



The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by operating system version on the computer

- *To filter or search for hosts with the Endpoint Sensors component based on the version of the operating system installed on the computer hosting the Endpoint Sensors component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**

- **KSC.**
3. Click the **OS** link to open the filter configuration window.
 4. In the drop-down list, select one of the following filtering operators:
 - **Contains.**
 - **Does not contain.**
 5. In the entry field, specify one or several characters of the operating system version.
 6. To add a filter condition using a different criterion, click  and specify the filter condition.
 7. If you want to delete the filter condition, click the  button to the right of the field.
 8. Click the **Apply** button.



The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors based on the Endpoint Sensor component version

- *To filter or search for hosts with the Endpoint Sensors component based on the version of the Endpoint Sensors component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the **Version** link to open the filter configuration window.
4. In the drop-down list, select one of the following filtering operators:
 - **Contains.**
 - **Does not contain.**
5. In the entry field, specify one or several characters of the version of the Endpoint Sensors component.
6. To add a filter condition using a different criterion, click  and specify the filter condition.
7. If you want to delete the filter condition, click the  button to the right of the field.

8. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors based on their activity

► *To filter or search for the Endpoint Sensors components based on their activity:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node**.
 - **KSC**.
3. Click the **Activity** link to open the filter configuration window.
4. Select the check boxes next to one or more Endpoint Sensors component activity indicators (see page [209](#)):
 - **Normal activity**, if you want to find hosts from which the last data was recently received.
 - **Warning**, if you want to find hosts from which the last data was received a long time ago.
 - **Critical inactivity**, if you want to find hosts from which the last data was received an extremely long time ago.
5. Click the **Apply** button.

The filter configuration window closes.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Filtering and searching Endpoint Sensors by operating errors of the component

If you are not using the distributed solution and multitenancy mode and are using a standalone Central Node server, you can filter or find hosts with the Endpoint Sensors component based on operating errors of the component.

- *To filter or find hosts with the Endpoint Sensors component based on operating errors of the component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of computers with the Endpoint Sensors component.
2. Click the **Errors** link to open the filter configuration window.
3. In the drop-down list, select one of the following options:
 - If you want the table to display all hosts with the Endpoint Sensors component, select **All**.
 - If you want the table to display only hosts on which the Endpoint Sensors component is running with errors, select **With errors**.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

You can use multiple filters at the same time.

Quickly creating a filter for computers with the Endpoint Sensors component


- *To quickly create a filter for hosts with the Endpoint Sensors component:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node**.
 - **KSC**.
3. Do the following to quickly add filter conditions to the filter being created:
 - a. Position the mouse cursor on the link containing the table column value that you want to add as a filter condition.
 - b. Left-click it.
This opens a list of actions to perform on the value.
 - c. In the list that opens, select one of the following actions:
 - **Filter by this value**, if you want to include this value in the filter condition.
 - **Exclude from filter**, if you want to exclude the value from the filter condition.
4. If you want to add several filter conditions to the filter being created, perform the actions to quickly add each filter condition to the filter being created.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

Clearing the Endpoint Sensors filter

► *To clear a filter for hosts with the Endpoint Sensors component based on one or multiple filter conditions:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
2. If distributed solution and multitenancy mode (see page [43](#)) is disabled, select one of the following subsections:
 - **Central Node.**
 - **KSC.**
3. Click the  button on the right of the header of the table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of hosts with the Endpoint Sensors component displays only hosts that match the conditions that you specified.

Configuring Endpoint Sensors activity indicators

Users with the **Local administrator** and **Administrator** permissions can define which period of inactivity of computers with the Endpoint Sensors component is considered to be normal, low, or very low activity, and can configure the activity indicators for Endpoint Sensors components. All users can view the activity indicators for Endpoint Sensors.

► *To configure activity indicators for Endpoint Sensors components:*

1. Sign in to the program web interface under the **Local administrator** or **Administrator** account.
2. In the window of the program web interface, select the **Settings** section, **Endpoint Sensors** subsection.
3. In the fields under the section name, enter the number of days of inactivity of computers with the Endpoint Sensors component that you want to display as **Warning** and **Critical inactivity**.
4. Click the **Apply** button.

Users with **Senior security officer** and **Security officer** permissions can see activity indicators that you configured for Endpoint Sensors components in the **Activity** field of the Endpoint Sensors host table in the **Endpoint Sensors** section of the program web interface.

Supported interpreters and processes

The Endpoint Sensors component monitors the execution of scripts by the following interpreters:

- cmd.exe;
- reg.exe;

- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msixexec.exe;
- mshta.exe;
- rundll32.exe;
- runlegacycplelevated.exe;
- control.exe;
- explorer.exe;
- regsvr32.exe;
- wwahost.exe;
- powershell.exe;
- java.exe and javaw.exe (only if started with the –jar option);
- InstallUtil.exe;
- msdt.exe;
- python.exe;
- ruby.exe;
- rubyw.exe.

Information about the processes monitored by the Endpoint Sensor component is presented in the table below.

Table 14. Processes and the file extensions that they open

Process	File extensions
winword.exe	rtf doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltn xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

Network isolation of hosts with the Endpoint Sensors component

Network isolation is available for hosts with Endpoint Sensors component version 3.5 or 3.6.

When a network isolation rule is enabled on a host, all current connections are disconnected and a VPN connection becomes unavailable.

The program blocks the connection of isolated hosts with an Active Directory server. If the operating system settings require a connection to Active Directory services for authorization, the user of an isolated host will not be able to log in to the system.

If the program administrator replaces the certificate of the server with the Central Node component (see [page 188](#)) while a network isolation rule is enabled, you cannot disable the rule.

To ensure correct operation of an isolated host, it is recommended to meet the following conditions:

- Create a local administrator account on the host or save the domain account data to the cache before enabling the network isolation rule.
- Do not change the certificate and IP address of the server with the Central Node component while the network isolation rule is enabled.

Isolated hosts can access the following resources over the network:

- Server with the Central Node component.
- Source of program database updates (Kaspersky Lab update server or custom source).
- Servers of the KSN service.
- Hosts added to network isolation rule exclusions.

If there is no connection between the isolated host and the server with the Central Node component for more than 5 hours, the network isolation rule is automatically disabled.

Creating a network isolation rule

► *To create a network isolation rule:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.

This will open the table of hosts with the Endpoint Sensors component.

2. Select the host for which you want to enable or disable the network isolation rule.
This opens a window containing information about the host.
3. Click the **Isolate** button.
4. In the **Exclusions to the host isolation rule** settings group, select the direction of network traffic that must not be blocked:
 - **Incoming/Outgoing.**
 - **Incoming.**
 - **Outgoing.**
5. In the **IP** field, enter the IP address whose network traffic must not be blocked.
6. If you selected **Incoming** or **Outgoing**, in the **Ports** field enter the connection ports.
7. If you want to add more than one exclusion, click the **Add** button and repeat steps 4–6.
8. Click the **Save** button.

The host will be isolated from the network.

You can also create a network isolation rule by clicking the **Host name** link in the event information (see page [267](#)) and in the alert information (see page [248](#)).

Adding an exclusion from a network isolation rule

► *To add an exclusion to a previously created network isolation rule:*

1. Select the **Endpoint Sensors** section in the window of the program web interface.
This will open the table of hosts with the Endpoint Sensors component.
2. Select the isolated host for which you want to create an exclusion from the network isolation rule.
This opens a window containing information about the host.
3. Click the **Add to exclusions** link to expand the **Exclusions to the host isolation rule** settings group.
4. Select the direction of network traffic that must not be blocked:
 - **Incoming/Outgoing.**
 - **Incoming.**
 - **Outgoing.**
5. In the **IP** field, enter the IP address whose network traffic must not be blocked.
6. If you selected **Incoming** or **Outgoing**, in the **Ports** field enter the connection ports.
7. If you want to add more than one exclusion, click the **Add** button and repeat steps 4–6.
8. Click the **Save** button.

The network isolation rule exclusion will be added.

Disabling a network isolation rule

To disable a network isolation rule:

1. Select the **Endpoint Sensors** section in the window of the program web interface.

This will open the table of hosts with the Endpoint Sensors component.

2. Select the host for which you want to disable the network isolation rule.

This opens a window containing information about the host.

3. Click the **Disable isolation** button.

The action confirmation window opens.

4. Click **Yes**.

5. In the window containing information about the host, click the **Close** button.

The network isolation rule will be disabled for the host.

Managing tasks

When working in the program web interface, users with the **Senior security officer** role can manage files and programs on hosts by creating and deleting tasks: **Kill process**, **Run program**, **Get file**, **Delete file**, **Quarantine file**, and **Restore file from Quarantine**.

The **Kill process**, **Run program**, **Delete file**, **Quarantine file**, and **Restore file from Quarantine** tasks may be one of the following types:

- **Local**—Created on the SCN server. These tasks apply only to hosts that are connected to this SCN server. Tasks belong to the organization for which the user is working in the program web interface (see page [230](#)) (if you are using distributed solution and multitenancy mode).
- **Global**—Created on the PCN server. These tasks apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Tasks belong to the organization for which the user is working in the program web interface (see page [230](#)).

The **Get file** task is run only on the specified host, regardless of the program management mode.

Users with the **Senior security officer** role can work with all tasks for the organizations whose data they can access (see page [160](#)).

Users with the **Security officer** role cannot access tasks.

The maximum task execution time is 24 hours. If the task did not complete in this time, execution is paused.

Viewing the task table

The tasks table contains a list of created tasks and is in the **Tasks** section of the program web interface window. You can view all tasks or only tasks created by you (current user).

► *To display only tasks created by the current user:*

turn on the **Only mine** switch in the upper right corner of the window.

The display of tasks created by the current user is enabled by default.

The tasks table contains the following information:

1. **Time created**—Task creation date and time.
2. **Type**—Type of task according to the task scope.

Tasks may be one of the following types:

- **Global**—Created on the PCN server. These tasks apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Tasks belong to the organization for which the user is working in the program web interface (see page [230](#)).
- **Local**—Created on the SCN server. These tasks apply only to hosts that are connected to this SCN server. Tasks belong to the organization for which the user is working in the program web interface (see page [230](#)) (if you are using distributed solution and multitenancy mode).

3. **Name**—Task name.

A task may have one of the following names:

- **Kill process.**

- **Run program.**
- **Get file.**
- **Delete file.**
- **Quarantine file.**
- **Restore file from Quarantine.**

Clicking the link with the name of the task type opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

4. **Details**—Full path to the file or data stream for which the task was created.

Clicking the link containing information about the path to the file or data stream opens a list in which you can select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Copy value to clipboard.**

5. **Servers**—Name of the server with the PCN or SCN role on which the task is run.

This field is displayed only if you are using distributed solution and multitenancy mode.

6. **Hosts**—Name of the host on which the task is run.

This field is displayed only if you are using a standalone Central Node server.

7. **Created by**—Name of the user who created the task.

If only tasks created by the current user are displayed, this column is not shown.

8. **State**—Task completion status.

A task can have one of the following statuses:

- **Pending.**
- **In process.**
- **Completed.**

Viewing information about a task

► *To view information about a task:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Select the task for which you want to view information.

This opens a window containing information about the task.

The window can contain the following information depending on the task type:

- **State**—Task completion status.
- **Description**—Task description.
- **File path**—Path to the file or data stream.
- **SHA256**—SHA256 hash of the file that you want to receive.
- **Command**—Program run command.
- **Working directory**—Working directory of the program.
- **Run as**—Program run parameter: on behalf of the current user or the local system name.
- **Created by**—Name of the user who created the task.
- **Company**—Name of the organization; it is displayed only when you are using distributed solution and multitenancy mode.
- **Time created**—Time when the task was created.
- **Time completed**—Task completion time.
- **Report**—Task result on selected hosts.

Creating a process termination task

If you believe that a process running on the computer could threaten the security of the computer or the corporate LAN, you can terminate the process.

► *To create a process termination task:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Add** button and select **Kill process**.
The task creation window opens.
3. Specify the following parameters:
 - a. **File path** —Path to the file of the process that you want to terminate.
You can also specify the path to an alternate data stream of this file. In this case, only processes of the specified data stream will be terminated. The processes of the other streams of this file will be executed.
 - b. **MD5/SHA256**—MD5- or SHA256 hash of the file of the process that you want to terminate. This field is optional.
 - c. **Description**—Task description. This field is optional.
 - d. If you want to display a task run notification to the user of the computer on which the task is running, select the **Notify user about the task execution** check box on the right of the **Notification** parameter name.
 - e. **Task for**—Task scope:
 - If you want to run the task on all hosts of all servers, select the **All hosts** option.

- If you want to run the task on selected servers, select the **Specified servers** option and on the right of the **Servers** parameter name select the check boxes next to the names of the servers on which you want to run the task.

This option is available only when distributed solution (see page 43) and multitenancy mode is enabled.

- If you want to run the task on selected hosts, select the **Specified hosts** option and list these hosts in the **Hosts** field.

4. Click the **Add** button.

The process termination task will be created.

Creating a program execution task

You can run a program startup task or command execution task.

If the standard output file or error output file reaches a size of 100 KB when the task is running, some of the data is deleted from the file. The file will not contain all the data.

► *To create a task for starting a program or executing a command:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **Add** button and select **Run program**.

The task creation window opens.

3. Specify the following parameters:

- a. If you want to run the program as SYSTEM, in the **Settings** settings group select the **Run as SYSTEM** check box.

The check box is cleared by default. The program will be run on behalf of the current user.

- b. Select one of the following actions:

- If you want to run a program using the command line (cmd.exe) or execute a command, select the **Execute command** option and type the command in the **Command** field.
- If you want to run a program directly, select the **Run a file** option, specify the full path to the file in the **File path** field and the startup keys in the **Arguments** field.

You can also specify the path to an alternate data stream of this file.

- c. **Description**—Task description. This field is optional.

- d. **Working directory**—Working directory of the program that you want to run.

- e. If you want to display a task run notification to the user of the computer on which the task is running, select the **Notify user about the task execution** check box on the right of the **Notification** parameter name.

- f. **Task for**—Task scope:

- If you want to run the task on all hosts of all servers, select the **All hosts** option.

- If you want to run the task on selected servers, select the **Specified servers** option and on the right of the **Servers** parameter name select the check boxes next to the names of the servers on which you want to run the task.

This option is available only when distributed solution and multitenancy mode is enabled.

- If you want to run the task on selected hosts, select the **Specified hosts** option and list these hosts in the **Hosts** field.

4. Click the **Add** button.

The program startup task or command execution task will be created.

Example:

► *To completely reject the network interfaces of a host by executing the command on behalf of the current user on all hosts, proceed as follows:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **Add** button and select **Run program**.

The task creation window opens.

3. Specify the following parameters:

a. In the **Settings** group, select the **Execute command** option and enter the command `netsh interface set interface <Interface name> admin=disable` in the **Command** field.

b. In the **Description** field, enter the task description.

c. Select the **All hosts** task scope.

4. Click the **Add** button.

Run the command for disabling each network interface.
Disable the network interface connecting the host with the Central Node component in the last turn.

After the task has been successfully performed, the host network interfaces will be disabled.

Creating a file download task

► *To create a file download task:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **Add** button and select **Get file**.

The task creation window opens.

3. Specify the following parameters:

- a. **File path**—Path to the file that you want to receive.

You can also specify the path to an alternate data stream of this file. In this case, you will receive only the specified stream.

- b. **MD5/SHA256**—MD5- or SHA256 hash of the file that you want to receive. This field is optional.

If this parameter is defined, more than one file may be received.

- c. If you do not want to scan the file, clear the **Send for scanning** check box.

The check box is selected by default.

- d. **Description**—Task description. This field is optional.

- e. **Host**—Host name or IP address of the server from which you want to receive the file.

4. Click the **Add** button.

The file download task will be created. A file received through this task will be placed in Backup.

If the file download task completed successfully, you can download the received file to your local computer.

► *To download the received file to the local computer:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Open the task for receiving the file that you want to download.
3. In the lower part of the **Get file** window, click the host name or IP address.
This opens a window containing information about the file.
4. Click the **Download** button.

The file will be saved to your local computer in the browser's downloads folder.

Creating a file deletion task

► *To create a file deletion task:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Add** button and select **Delete file**.
The task creation window opens.
3. Specify the following parameters:
 - a. **File path**—Path to the file that you want to delete.
You can also specify the path to an alternate data stream of this file. In this case, only the specified data stream will be deleted. The other data streams of this file will be left unchanged.
 - b. **MD5/SHA256**—MD5- or SHA256 hash of the file that you want to delete. This field is optional.
 - c. **Description**—Task description. This field is optional.

- d. If you want to display a task run notification to the user of the computer on which the task is running, select the **Notify user about the task execution** check box on the right of the **Notification** parameter name.

e. **Task for**—Task scope:

- If you want to run the task on all hosts of all servers, select the **All hosts** option.
- If you want to run the task on selected servers, select the **Specified servers** option and on the right of the **Servers** parameter name select the check boxes next to the names of the servers on which you want to run the task.

This option is available only when distributed solution and multitenancy mode is enabled.

- If you want to run the task on selected hosts, select the **Specified hosts** option and list these hosts in the **Hosts** field.

4. Click the **Add** button.

The file deletion task will be created.

If the file has been blocked by another process, the task will be displayed with the *Completed* status but the file will be deleted only after the host is restarted. It is recommended to check whether the file is successfully deleted after the host is restarted.
Deleting the file from a mapped network drive is not supported.

Creating a file quarantine task

If you believe that an infected or probably infected file is on the computer, you can isolate it by putting it into Quarantine.

► *To create a file quarantine task:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Add** button and select **Quarantine file**.
The task creation window opens.
3. Specify the following parameters:
 - a. **File path**—Path to the file that you want to put in Quarantine.
 - b. **MD5/SHA256**—MD5- or SHA256 hash of the file that you want to place in Quarantine. This field is optional.
 - c. If you do not want to scan the file, clear the **Send for scanning** check box.
The check box is selected by default.
 - d. **Description**—Task description. This field is optional.
 - e. If you want to display a task run notification to the user of the computer on which the task is running, select the **Notify user about the task execution** check box on the right of the **Notification** parameter name.
 - f. **Host**—Names of the hosts from which you want to delete the file after putting a copy of it in Quarantine.

4. Click the **Add** button.

The file quarantine task will be created. As a result of the task, the file will be deleted from the selected hosts and placed in Quarantine.

If the file has been blocked by another process, the task will be displayed with the Completed status but the file will be placed in Quarantine only after the host is restarted. It is recommended to check whether the task was successfully completed after the host is restarted.

Creating a quarantined file recovery task

If you believe that a previously isolated file is safe, you can restore it from Quarantine to the host.

► *To create a task for restoring a file from Quarantine:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Add** button and select **Restore file from Quarantine**.
The task creation window opens.
3. Specify the following parameters:
 - a. **Description**—Task description. This field is optional.
 - b. If you want to display a task run notification to the user of the computer on which the task is running, select the **Notify user about the task execution** check box on the right of the **Notification** parameter name.
 - c. **File search**—Name of the file in Quarantine.
4. Click the **Add** button.

The task for restoring a file from Quarantine will be created.

After restoring a file from Quarantine to a host, metadata about the file remains in the table of objects placed in Storage.

Creating a copy of a task

► *To copy a task:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Open the task that you want to copy.
3. Click the **Duplicate** button.
The task creation window opens. All task settings will be copied.
4. Click the **Add** button.

A copy of the selected task will be created.

Deleting a task

If you delete a task while it is running, the task results might not be saved.
If you delete a successfully completed file download task, the file will be deleted.

► To delete a task:

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Open the task that you want to delete.
3. Click the **Delete** button.

The action confirmation window opens.

4. Click **Yes**.

The task will be deleted.

Filtering tasks by creation time

► To filter tasks based on their creation time:

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **Time created** link to open the task filtering menu.

3. Select one of the following task display periods:

- **All**, if you want the program to display all created tasks in the table.
- **Last hour**, if you want the program to display the tasks that were created during the last hour in the table.
- **Last day**, if you want the program to display the tasks that were created during the last day in the table.
- **Custom range**, if you want the program to display tasks that were created during the period you specify in the table.

4. If you have selected the **Custom range** task display period:

- a. In the calendar that opens, specify the start and end dates of the task display period.
- b. Click the **Apply** button.

The calendar closes.

The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks by type

If you are using distributed solution and multitenancy mode, you can filter tasks by their type.

► *To filter tasks by type:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Type** link to open the task filtering menu.
3. Select one of the following task display options:
 - **All**, if you want to display all tasks regardless of their type.
 - **Global**, if you want to display only tasks that were created on the PCN server. These tasks apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Tasks belong to the organization for which the user is working in the program web interface (see page [230](#)).
 - **Local**, if you want to display only tasks that were created on a SCN server. These tasks apply only to hosts that are connected to this SCN server. Tasks belong to the organization for which the user is working in the program web interface (see page [230](#)) (if you are using distributed solution and multitenancy mode).

The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks by name

► *To filter tasks by name:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Name** link to open the task filtering menu.
3. Select one or several check boxes:
 - **Get file.**
 - **Kill process.**
 - **Delete file.**
 - **Quarantine file.**
 - **Restore file.**
 - **Run program.**
4. Click the **Apply** button.


The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks by file name and path

You can filter tasks based on the **Details** criterion—Name and path to the file or data stream.

► *To filter tasks based on the name and path to the file or data stream:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Details** link to open the task filter configuration window.
3. In the drop-down list on the right, select **Details**.
4. In the drop-down list on the left, select one of the following task filtering operators:
 - **Contains.**
 - **Does not contain.**
 - **Equal to.**
 - **Not equal to.**
5. In the entry field, specify one or several characters of the file name or path.
6. To add a filter condition using a different criterion, click  and specify the filter condition.
7. Click the **Apply** button.

The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks by description

You can filter tasks by the **Description** criterion, which is the task description that was added when the task was created.

► *To filter tasks by description:*

1. Select the **Tasks** section in the program web interface window.
The tasks table opens.
2. Click the **Details** link to open the task filter configuration window.
3. In the drop-down list on the left, select **Description**.
4. In the drop-down list on the right, select one of the following task filtering operators:
 - **Contains.**
 - **Does not contain.**
 - **Equal to.**

- **Not equal to.**

5. In the entry field, specify one or several characters of the file name or path.

6. To add a filter condition using a different criterion, click  and specify the filter condition.

7. Click the **Apply** button.

The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks by server name

If you are using distributed solution and multitenancy mode, you can filter tasks based on the servers to which the tasks are applied.

► *To filter tasks based on the servers to which the tasks are applied:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **Servers** link to open the task filtering menu.

3. Select the check boxes next to the names of the servers whose tasks you want to display.

The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks based on the name of the user that created the task

To filter tasks based on the user name that created the task, all tasks must be displayed. If only tasks created by the current user are displayed, tasks cannot be filtered by user name.

► *To filter tasks based on the name of the user that created the task:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **Created by** link to open the task filtering menu.

3. In the drop-down list, select one of the following task filtering operators:

- **Contains.**
- **Does not contain.**

4. In the entry field, specify one or several characters of the user name.

5. To add a filter condition using a different criterion, click  and specify the filter condition.

6. Click the **Apply** button.

The tasks table displays only tasks matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering tasks by processing status

► *To filter tasks based on their user processing status:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the **State** link to open the task filtering menu.

3. Select one or several check boxes:

- **Pending.**
- **In process.**
- **Completed.**

4. Click the **Apply** button.

The tasks table displays only tasks matching the filter criteria you have set.


You can use multiple filters at the same time.

Clearing a task filter

► *To clear a task filter based on one or multiple filter conditions:*

1. Select the **Tasks** section in the program web interface window.

The tasks table opens.

2. Click the  button on the right of the header of the table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The tasks table displays only tasks matching the filter criteria you have set.

Managing policies (prevention rules)

When working in the program web interface, users with the **Senior security officer** role can use policies to manage prevention rules for files and processes on selected hosts. For example, you can prevent the startup of applications that you consider unsafe to use on the selected host with the Endpoint Sensors component. The program identifies files based on their hash by using the MD5 and SHA256 hashing algorithms. You can create, delete and edit preventions.

Prevention rules can have the following types:

- **Local**—Created on the SCN server. These prevention rules apply only to hosts that are connected to this SCN server. Prevention rules belong to the organization for which the user is working in the program web interface (if you are using distributed solution and multitenancy mode).
- **Global**—Created on the PCN. These prevention rules apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Prevention rules belong to the organization for which the user is working in the program web interface (see page [230](#)).

Users with the **Senior security officer** role can create, edit, delete, enable and disable prevention rules for the organizations whose data they can access (see page [160](#)).

Users with the **Security officer** role cannot access prevention rules.

All changes to prevention rules are applied on hosts after an authorized connection is established with the selected hosts. If there is no connection with the hosts, the old prevention rules continue to be applied on the hosts. Changes to prevention rules do not affect processes that are already running.

If an attempt to run a file is made before the Endpoint Sensors component is started or after the Endpoint Sensors component is shut down on a host, the file will be blocked from running. The user's computer will display a notification about the blocked file run when the Endpoint Sensors component is started.

You can create only one prevention rule for each file hash.

Viewing the prevention rule table

The table of prevention rules is in the **Prevention** section of the program web interface window.

The table contains the following information:

1. **Type**—Type of prevention rule. Prevention rules can have the following types:
 - **Global**—Created on the PCN. These prevention rules apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Prevention rules belong to the organization for which the user is working in the program web interface (see page [230](#)).
 - **Local**—Created on the SCN server. These prevention rules apply only to hosts that are connected to this SCN server. Prevention rules belong to the organization for which the user is working in the program web interface (if you are using distributed solution and multitenancy mode).
2. **Name** is the name of the prevention rule.
3. **Servers** refer to the names of the servers with the PCN or SCN role to which the prevention rule is applied (if you are using distributed solution and multitenancy mode).

This field is displayed only when you are using distributed solution and multitenancy mode.

4. **Hosts** is the name of the server with the Central Node component to whose hosts the prevention rule is applied.

This field is displayed only when you are using a standalone Central Node server.

5. **File hash**—Hashing algorithm applied to identify a file.

A file can be identified based on one of the following hashing algorithms:

- **MD5.**
- **SHA256.**

Clicking the link with the name of the hashing algorithm opens a list in which you can view the file hash and select one of the following actions:

- **Filter by this value.**
- **Exclude from filter.**
- **Find on Kaspersky Threat Intelligence Portal.**
- **Find on virustotal.com.**
- **Find events.**

When this action is performed, the **Threat Hunting** section opens with events that are already filtered based on the hash you selected.

- **Enable prevention rule.**
- **Disable prevention rule.**
- **Delete prevention rule.**
- **Copy value to clipboard.**

6. **State** is the current state of the prevention rule.

A prevention rule can have one of the following states:

- **Enabled**
- **Disabled**

Viewing a prevention rule

► *To view information about a prevention rule:*

1. Select the **Prevention** section in the program web interface window.

The prevention rule table opens

2. Select the prevention rule that you want to view.

A prevention rule contains the following information:

- The **Events** link opens the **Threat Hunting** section with the search condition containing your selected prevention rule.
- **State** is the current state of the prevention rule.

A prevention rule can have one of the following states:

- **Enabled**
- **Disabled**
- The **Details** tab contains the following information:
 - **MD5/SHA256** is the hash of the file prevented from running.
 - **Name** is the name of the prevention rule or file prevented from running.
 - **Type**—Type of prevention rule. Prevention rules can be one of the following types:
 - **Global**—Created on the PCN. These prevention rules apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Prevention rules belong to the organization for which the user is working in the program web interface (see page [230](#)).
 - **Local**—Created on the SCN server. These prevention rules apply only to hosts that are connected to this SCN server. Prevention rules belong to the organization for which the user is working in the program web interface (if you are using distributed solution and multitenancy mode).
 - **Notification** is the state of the **Notify user about the task execution** setting.
 - **Prevent on** is the list of hosts on which the prevention rule is applied.
If the prevention is in effect on all hosts, the **All hosts** section is displayed.
- The **Change log** tab contains a list of changes made to the prevention: time of the change, name of the user that changed the prevention, and actions taken on the prevention.

Creating a prevention rule

► *To create a prevention rule:*

1. Select the **Prevention** section in the program web interface window.
The prevention rule table opens
2. Click the **Add** button.
The prevention rule creation window opens.
3. Specify the following parameters:
 - a. **State** is the state of the prevention rule:
 - b. If you want to enable the prevention rule, set the toggle switch to **On**.
 - c. If you want to disable the prevention rule, set the toggle switch to **Off**.
 - d. **MD5/SHA256**—MD5- or SHA256 hash of the file or data stream that you want to prevent from starting.
 - e. **Name** is the name of the prevention rule.
 - f. If you want the program to show a prevention rule triggering notification to the user of the computer on which the prevention is applied, select the **Notify user about the task execution** check box.
 - g. **Prevent on** is the prevention rule scope:
 - If you want to apply the prevention rule on all hosts of all servers, select **All hosts**.
 - If you want to apply the prevention rule on selected servers, select the **Specified servers** option and on the right of the **Servers** parameter name select the check boxes next to the names of the servers on which you want to apply the prevention rule.

This option is available only when distributed solution and multitenancy mode is enabled.

- If you want to apply the prevention rule on selected hosts, select the **Specified hosts** option and list these hosts in the **Hosts** field.

4. Click the **Add** button.

The file startup prevention will be created.

If you selected the **Notify user about the task execution** check box and there is an attempt to start a file prevented from running, the user will be notified that a startup prevention rule was triggered by this file.

Enabling and disabling a prevention

► *To enable or disable a prevention rule:*

1. Select the **Prevention** section in the program web interface window.

The prevention rule table opens

2. In the row containing the prevention rule that you want to enable or disable, in the **State** column perform one of the following actions:

- If you want to enable the prevention rule, set the toggle switch to **Enabled**.

The prevention rule you selected will be enabled.

- If you want to disable the prevention rule, set the toggle switch to **Disabled**.

The prevention rule you selected will be disabled.

Deleting a prevention rule

► *To delete a prevention rule:*

1. Select the **Prevention** section in the program web interface window.

The prevention rule table opens

2. Click the prevention rule that you want to delete.

The prevention rule details window opens.

3. Click the **Delete** button.

The action confirmation window opens.

4. Click **Yes**.


The prevention rule will be deleted.

Filtering preventions by name

► *To filter preventions by name:*

1. Select the **Prevention** section in the program web interface window.

The prevention rule table opens

2. Click the **Name** link to open the prevention filtering menu.
3. In the drop-down list, select one of the following prevention filtering operators:
 - **Contains.**
 - **Does not contain.**
4. In the entry field, specify one or several characters of the prevention name.
5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.

The prevention rules table displays only the prevention rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering prevention rules by type

If you are using distributed solution and multitenancy mode, you can prevention rules by their type.

► *To filter prevention rules by type:*

1. Select the **Prevention** section in the program web interface window.
The prevention rule table opens
2. Click the **Type** link to open the prevention rule filtering menu.
3. Select one of the following options for displaying prevention rules:
 - **All**, if you want to display all prevention rules regardless of their type.
 - **Global**, if you want to display only the prevention rules that were created on the PCN. These prevention rules apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Prevention rules belong to the organization for which the user is working in the program web interface (see page [230](#)).
 - **Local**, if you want to display only prevention rules that were created on a SCN server. These prevention rules apply only to hosts that are connected to this SCN server. Prevention rules belong to the organization for which the user is working in the program web interface (if you are using distributed solution and multitenancy mode).

The prevention rules table displays only the prevention rules that match the filter criteria you have set.


You can use multiple filters at the same time.

Filtering preventions by file hash

► *To filter preventions by file hash:*

1. Select the **Prevention** section in the program web interface window.

The prevention rule table opens

2. Click the **File hash** link to open the prevention filtering menu.
3. In the drop-down list, select one of the following prevention filtering operators:
 - **Contains.**
 - **Does not contain.**
4. In the entry field, specify one or several characters of the file hash.
5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.

The prevention rules table displays only the prevention rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering preventions by server name

If you are using distributed solution and multitenancy mode, you can filter prevention rules based on the servers to which the prevention rules apply.

► To filter prevention rules by server name:


1. Select the **Prevention** section in the program web interface window.
The prevention rule table opens
2. Click the **Servers** link to open the prevention rule filtering menu.
3. Select the check boxes next to those servers by which you want to filter the prevention rules.
4. Click the **Apply** button.

The prevention rules table displays only the prevention rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Clearing a prevention rule filter

► To clear a prevention rules filter based on one or multiple filter conditions:

1. Select the **Prevention** section in the program web interface window.
The prevention rule table opens
2. Click the  button on the right of the header of the prevention rules table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The prevention rules table displays only the prevention rules that match the filter criteria you have set.

Managing indicators of compromise and attack

Kaspersky Anti Targeted Attack Platform uses two types of indicators for threat hunting: *IOC* (Indicator of Compromise) and *IOA* (Indicator of Attack).

An IOC is a set of data about a malicious object or malicious activity. Kaspersky Anti Targeted Attack Platform uses IOC files conforming to the OpenIOC standard, which is an open standard for describing indicators of compromise. IOC files contain a set of indicators that are compared to the indicators of an event. If the compared indicators match, the program considers the event to be an alert. The likelihood of an alert may increase if a scan detects exact matches between the data of an object and several IOC files.

An IOA (also referred to as an IOA rule) is a rule containing the description of a suspicious activity in the system that could be a sign of a targeted attack. Kaspersky Anti Targeted Attack Platform scans the event database (see page [260](#)) of the program and marks events that match behaviors described by IOA rules. The *streaming scan* technology is used, which involves continuous real-time scanning of objects downloaded from the network.

IOA rules created by experts at Kaspersky Labs are updated together with program databases. They are not displayed in the interface of the program and cannot be edited. You can add custom IOA rules (see page [328](#)) in the form of IOC files conforming to the OpenIOC standard, and create IOA rules based on conditions for searching the events database (see page [265](#)).

The following table contains a comparative analysis of IOC and IOA indicators.

Table 15 Comparison of IOC and IOA indicators

Characteristic	IOC	IOA
Scan scope	Computers with the Endpoint Sensors component	Program events database
Scanning mechanism	Periodical scan	Streaming scan
Predefined indicators by Kaspersky Lab experts	None	Yes
Ability to add to a white list	None	Yes

If you are using the distributed solution and multitenancy mode, the section displays data on the organization that you chose (see page [230](#)).

IOC scan of events

When working in the program web interface, users with the **Senior security officer** and **Security officer** role can use IOC files to search for signs of targeted attacks, infected and probably infected objects in the database of events and alerts, and to scan local computers that have the Endpoint Sensors component installed.

Depending on the program operating mode and the server to which the IOC files are uploaded, the uploaded files can be one of the following types:

- **Local**—Uploaded to a SCN server. These IOC files are used to scan events on this SCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).
- **Global**—Uploaded to the PCN server. These IOC files are used to scan events on this PCN server and on all SCN servers connected to this PCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).

Users with the **Senior security officer** role can manage scans of events based on IOC files: add, edit, delete, and download IOC files to the computer, enable and disable scanning of events based on IOC files, and manage object scan settings.





Users with the **Security officer** role can only view information about IOC files and download IOC files to a computer.

If you are working with events that were previously detected by the program, a repeated match between the data of these events and indicators of compromise does not always indicate a possible alert.

Viewing the table of IOC files

The table of IOC files contains information about IOC files used for scanning on computers with the Endpoint Sensors component installed; you can find the table in the **IOC/IOA Analysis** section, **IOC Scanner** subsection of the program web interface window.

The table of IOC files contains the following information:

1. —Importance level that will be assigned to an alert generated using this IOC file.
The importance level can have one of the following values:
 - —Low importance.
 - —Medium importance.
 - —High importance.
2. **Type**—Type of uploaded IOC file depending on the application operating mode and the server on which the IOC file was uploaded. IOC files can be one of the following types:
 - **Global**—Uploaded to the PCN server. These IOC files are used to scan events on this PCN server and on all SCN servers connected to this PCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).
 - **Local**—Uploaded to a SCN server. These IOC files are used to scan events on this SCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).
3. **Name**—Name of the IOC file.
4. **Servers**—Name of the server with the Central Node component on which events were scanned based on this IOC file.
5. **Autoscan**—Use of an IOC file during an automatic scan of events.
Event scanning using this IOC file can have one of the following statuses:
 - **Enabled**
 - **Disabled**

Viewing information about an IOC file

► To view information about an IOC file:

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.

The table of IOC files opens.




2. Select the IOC file for which you want to view information.

This opens a window containing information about the IOC file.

The window contains the following information:

- **Find alerts.** Clicking the link opens the **Alerts** section with the filter condition containing your selected IOC file.
- **Find events.** Clicking the link opens the **Threat Hunting** section with the search condition containing your selected IOC file.
- **Download file.** Clicking the link opens the IOC file download window.
- **Autoscan**—Use of an IOC file during an automatic scan of events.

Event scanning using this IOC file can have one of the following statuses:

- **Enabled**
- **Disabled**
- **Name**—Name of the IOC file.
- **Importance**—Importance level that will be assigned to an alert generated using this IOC file.
The importance level can have one of the following values:
 -  —Low importance.
 -  —Medium importance.
 -  —High importance.
- **Apply to.** Displays the name of the organization and the names of servers associated with events scanned based on this IOC file (in the distributed solution and multitenancy mode).
- **XML.** Displays the IOC file contents in XML format.

Uploading an IOC file

IOC files having UserItem properties for domain users are not supported.

► To upload an IOC file:

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.

The table of IOC files opens.

2. Click the **Upload** button.

The file selection window opens on your local computer.

3. Select the file that you want to upload and click the **Open** button.
4. Specify the following parameters:
 - a. **Autoscan**—Use of an IOC file during an automatic scan of events:
 - **Enabled**
 - **Disabled**
 - b. **Name**—Name of the IOC file.
 - c. **Importance**—Importance level that will be assigned to an alert generated using this IOC file:
 - **Low.**
 - **Medium.**
 - **High.**
 - d. **Apply to**—Name of the organization and names of the servers on which you want to scan events based on this IOC file (in the distributed solution and multitenancy mode).
5. Click the **Save** button.

The IOC file will be uploaded in XML format.

Downloading an IOC file to a computer

You can download a previously uploaded IOC file to a computer.

► *To download an IOC file to a computer:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.
The table of IOC files opens.
2. Select the IOC file that you want to download.
This opens a window containing information about the IOC file.
3. Depending on your browser settings, click the **Download file** link to save the file to the default folder or specify a folder in which to save the file.

The IOC file will be saved to the computer in the browser's downloads folder.

Enabling and disabling the automatic use of an IOC file when scanning events

You can enable or disable the automatic use of an IOC file when scanning events.

► *To enable or disable the automatic use of an IOC file when scanning events:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.
The table of IOC files opens.
2. In the line containing the IOC file whose use you want to enable or disable, in the **Autoscan** column, set the toggle switch to one of the following positions:
 - **Enabled**
 - **Disabled**
3. Click the **Save** button.

Automatic use of an IOC file when scanning events will be enabled or disabled.

Deleting an IOC file

► *To delete an IOC file:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.
The table of IOC files opens.
2. Select the IOC file that you want to delete.
This opens a window containing information about the IOC file.
3. Click the **Delete** button.
The IOC file will be deleted.

Searching IOC scan results

► *To find and view results of an IOC scan:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.
The table of IOC files opens.
2. Select the IOC file for which you want to view scan results.
This opens a window containing information about the IOC file.
3. Do one of the following:
 - If you want to view alerts generated by the IOC file, click **Find alerts** to proceed to the alerts database.
The alert table is opened in a new browser tab.
 - If you want to view events generated by the IOC file, click **Find events** to proceed to the events database.
The event table is opened in a new browser tab.

Filtering and searching IOC files

► *To filter or search for IOC files based on required criteria:*


1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.
The table of IOC files opens.
2. Depending on the filtering criterion, do the following:
 - **By importance**
 - **By file name**
 - **By server name**
 - **By state of IOC files**

The table of IOC files will display only IOC files that match the filter criteria you have set.

You can use multiple filters at the same time.

Clearing an IOC file filter

► *To clear an IOC file filter based on one or more filter conditions:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOC Scanner** subsection.
The table of IOC files opens.
2. Click the  button on the right of the header of the IOC files table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of IOC files will display only IOC files that match the filter criteria you have set.

Configuring an IOC scan schedule

You can configure an IOC scan schedule for computers on which the Endpoint Sensors component is installed.

► *To configure an IOC scan schedule:*

1. In the window of the program web interface, select the **Settings** section, **IOC scanning schedule** subsection.
2. In the **Start time** drop-down lists, select the scan start time.
3. In the **Time limit** drop-down list, select a time limit for completing the scan.
If a scan does not complete within the specified amount of time, some events may not be found.
4. Click the **Save** button.

The new IOC scan schedule will take effect immediately after the changes are saved. IOC scan results will be displayed in the alerts table.

Supported OpenIOC Indicators of Compromise

Kaspersky Anti Targeted Attack Platform supports the OpenIOC open standard indicators of compromise shown in the table below.

Table 16. Supported Indicators of Compromise

OpenIOC Indicator of Compromise	Implementation Limitations (if any)
FileItem/FileName	No value.
FileItem/Md5sum	No value.
FileItem/FilePath	Disclosure of user-specific environment variables is not supported. For example, %APPDATA%, %UserName%.
FileItem/SizeInBytes	No value.
RegistryItem/KeyPath	No value.
RegistryItem/Path	Scanning user-specific keys through HKEY_CURRENT_USER and HKEY_CLASSES_ROOT is not supported for unauthorized users.
RegistryItem/Value	No value.
FileItem/PEInfo/PETimeStamp	No value.
FileItem/FullPath	Disclosure of user-specific environment variables is not supported. For example, %APPDATA%, %UserName%.
PortItem/remotelP	No value.
FileItem/PEInfo/DetectedAnomalies/string	checksum_is_zero is only supported.
FileItem/FileExtension	No value.
DnsEntryItem/RecordName	No value.
ProcessItem/name	No value.
RegistryItem/ValueName	No value.
RegistryItem/Text	No value.
ServiceItem/name	No value.
FileItem/PEInfo/Exports/ExportedFunctions/string	No value.
FileItem/PEInfo/Exports/DllName	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/OriginalFilename	No value.
FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileDescription	No value.
ProcessItem/arguments	No value.
PortItem/remotePort	No value.
DnsEntryItem/RecordData/IPv4Address	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/InternalName	No value.
FileItem/PEInfo/Exports/NumberOfFunctions	No value.

OpenIOC Indicator of Compromise	Implementation Limitations (if any)
FileItem/PEInfo/DigitalSignature/SignatureExists	No value.
ProcessItem/SectionList/MemorySection/Name	No value.
FileItem/PEInfo/Type	No value.
ProcessItem/path	No value.
PortItem/localPort	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/CompanyName	No value.
ProcessItem/SectionList/MemorySection/Md5sum	No value.
DnsEntryItem/Host	No value.
PortItem/protocol	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductName	No value.
ServiceItem/description	No value.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Name	No value.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Language	No value.
ServiceItem/descriptiveName	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Language	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalCopyright	No value.
FileItem/PEInfo/ImportedModules/Module/Name	No value.
ServiceItem/serviceDLL	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileVersion	No value.
FileItem/PEInfo/Sections/Section/Name	No value.
FileItem/PEInfo/DigitalSignature/SignatureVerified	No value.
ServiceItem/path	No value.
FileItem/PEInfo/Subsystem	No value.
FileItem/Sha256sum	No value.
RegistryItem/Type	No value.
FileItem/PEInfo/DigitalSignature/CertificateSubject	No value.
EventLogItem/EID	No value.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Type	No value.
VolumItem/Name	No value.
EventLogItem/source	No value.
PortItem/state	No value.

OpenIOC Indicator of Compromise	Implementation Limitations (if any)
UserItem/Username	Local users are only scanned. Scanning domain users is not supported.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductVersion	No value.
DnsEntryItem/RecordType	No value.
VolumeItem/VolumeName	No value.
PortItem/localIP	No value.
ProcessItem/parentpid	No value.
FileItem/PEInfo/DigitalSignature/CertificateIssuer	No value.
ProcessItem/SectionList/MemorySection/Protection	No value.
ProcessItem/SectionList/MemorySection/Sha256sum	No value.
FileItem/PEInfo/Exports/ExportsTimeStamp	No value.
ProcessItem/Username	No value.
ServiceItem/status	No value.
ArpEntryItem/CacheType	No value.
ArpEntryItem/IPv4Address	No value.
ArpEntryItem/Interface	No value.
ArpEntryItem/PhysicalAddress	No value.
DnsEntryItem/DataLength	No value.
DnsEntryItem/Flags	No value.
DnsEntryItem/RecordData/Host	No value.

OpenIOC Indicator of Compromise	Implementation Limitations (if any)
DnsEntryItem/RecordName	No value.
DnsEntryItem/TimeToLive	No value.
VolumItem/ActualAvailableAllocationUnits	No value.
VolumItem/BytesPerSector	No value.
VolumItem/CreationTime	No value.
VolumItem/DevicePath	No value.
VolumItem/DriveLetter	No value.
VolumItem/FileSystemFlags	No value.
VolumItem/FileSystemName	No value.
VolumItem/IsMounted	No value.
VolumItem/SectorsPerAllocationUnit	No value.
VolumItem/SerialNumber	No value.
VolumItem/TotalAllocationUnits	No value.
VolumItem/Type	No value.
UserItem/LastLogin	No value.
UserItem/SecurityID	No value.
UserItem/SecurityType	No value.
UserItem/description	No value.
UserItem/disabled	No value.
UserItem/fullname	No value.
UserItem/homedirectory	No value.
UserItem/lockedout	No value.
UserItem/passwordrequired	No value.
UserItem/scriptpath	No value.
UserItem/userpasswordage	No value.
PortItem/CreationTime	No value.
PortItem/path	No value.
PortItem/pid	No value.
PortItem/process	No value.
EventLogItem/log	No value.
EventLogItem/index	No value.
EventLogItem/user	No value.

OpenIOC Indicator of Compromise	Implementation Limitations (if any)
EventLogItem/genTime	No value.
EventLogItem/machine	No value.
EventLogItem/CorrelationActivityId	No value.
EventLogItem/CorrelationRelatedActivityId	No value.
EventLogItem/ExecutionProcessId	No value.
EventLogItem/ExecutionThreadId	No value.
RegistryItem/Hive	Scanning user-specific keys through HKEY_CURRENT_USER and HKEY_CLASSES_ROOT is not supported for unauthorized users.
ServiceItem/pid	No value.
ServiceItem/type	No value.
ServiceItem/startedAs	No value.
ServiceItem/arguments	No value.
ServiceItem/mode	No value.
ProcessItem/pid	No value.
ProcessItem/startTime	No value.
ProcessItem/SectionList/MemorySection/RegionSize	No value.
ProcessItem/SectionList/MemorySection/RegionStart	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Comments	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalTrademarks	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/PrivateBuild	No value.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/SpecialBuild	No value.
FileItem/PEInfo/BaseAddress	No value.
FileItem/PEInfo/Exports/NumberOfNames	No value.
FileItem/PEInfo/ImportedModules/Module/NumberOfFunctions	No value.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Size	No value.
FileItem/PEInfo/Sections/ActualNumberOfSections	No value.
FileItem/PEInfo/Sections/NumberOfSections	No value.
FileItem/PEInfo/Sections/Section/SizeInBytes	No value.

IOA analysis of events

The program analyzes events using IOA rules. Kaspersky Lab experts provide a set of IOA rules which contain samples of the most frequent suspicious actions in the user's system. In addition, users can create their own IOA rules.

The web interface of the program allows users with the **Senior security officer** role to manage IOA rules: add (see page [328](#)), delete (see page [329](#)), enable and disable the rules (see page [327](#)), and add IOA rules by Kaspersky Lab to the white list (see page [331](#)). Users with the **Senior security officer** or **Security officer** roles can use IOC rules to search for signs of targeted attacks (see page [333](#)), infected and possibly infected objects in the database of events and alerts, and to view the IOA rule table (see page [326](#)) and IOA rule information (see page [326](#)).

The differences between user rules and Kaspersky Lab rules are summarized in the following table.

Table 17. Comparison of IOA rules

Characteristic	User rules	Kaspersky Lab rules
Recommendations on responding to the event	None	Yes You can view recommendations in alert information (see page 250)
Correspondence to technique in MITRE ATT&CK database	None	Yes You can view the description of the technique according to the MITRE database in alert information (see page 250)
IOA rule table (see page 326) display	Yes	None
Ability to disable database lookup for this rule	Disable rule (see page 327)	Add rule to white list (see page 331)
Ability to delete or add the rule	You can delete (see page 329) or add a rule (see page 328) in the web interface of the program	Rules are updated together with program databases and cannot be deleted by the user
Viewing the IOA analysis results (see page 333)	Using Alerts and Events links in the IOA rule information window (see page 326)	Using Alerts and Events links in the alert information window (see page 248)





Depending on the program operating mode and the server on which the IOA rules are created, custom IOA rules can be one of the following types:

- **Local**—Created on the SCN server. These IOA rules are used to scan events on this SCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).
- **Global**—Created on the PCN server. These IOA rules are used to scan events on this PCN server and all SCN servers connected to this PCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).

Viewing the IOA rule table

The IOA rule table contains information on IOA rules used to scan the events database. This table is located in the **IOC/IOA Analysis** section, **IOA Analysis** subsection of the program web interface window.

The table of IOA files contains the following information:

1.  is the level of importance that is assigned to an alert generated using this IOA rule.
The importance level can have one of the following values:
 -  – **Low**.
 -  – **Medium**.
 -  – **High**.
2. **Type** is the type of the rule depending on the role of the server on which it was generated, in distributed solution and multitenancy (see page [43](#)) mode:
 - **Global** – the rule was created on the PCN server.
 - **Local** – the rule was created on an SCN server.
3. **Confidence** – level of confidence depending on the likelihood of false alarms caused by the rule:
 - **High**.
 - **Medium**.
 - **Low**.

The higher the confidence, the lower the likelihood of false alarms.
4. **Name** – name of the rule.
5. **Servers** – name of the server with the Central Node component on which the rule is applied.
6. **Generate alerts** – requirement to store information on alerts based on matching an event from the database with criteria of the rule.
 - **Enabled** – a record is created for the event in the alerts table with IOA technology specified.
 - **Disabled** – not displayed in the alert table.
7. **State** – use of the rule in events database scans:
 - **Enabled** – the rule is being used.
 - **Disabled** – the rule is not being used.

Viewing information about an IOA rule

► *To view information about an IOA rule:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. Select the IOA rule whose information you want to view.
This opens a window containing information about the IOA rule.

The window contains the following information:

- **Events.** Clicking the link opens the **Threat Hunting** section with the search condition containing the selected IOA rule.
- **Alerts.** Clicking the link opens the **Alerts** section with the filter condition containing the selected IOA rule.
- **IOA ID.** Clicking this link shows the ID that the program assigns to each rule.
IDs cannot be modified. You can copy the ID by clicking the **Copy value to clipboard** button.
- **State** – use of the rule in events database scans.

The **Details** tab shows the following information:

- **Name** is the name of the rule that you specified when you added the rule.
- **Description** is any additional information about the rule that you specified.
- **Importance** is an estimate of the probable impact of the event on the security of computers or the corporate LAN as specified by the user when the rule was added.
- **Confidence** is the level of confidence depending on the likelihood of false alarms as defined by the user when the rule was added.
- **Type** is the type of the rule depending on the role of the server which generated it:
 - **Global**—Created on the PCN server. These IOA rules are used to scan events on this PCN server and all SCN servers connected to this PCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).
 - **Local**—Created on the SCN server. These IOA rules are used to scan events on this SCN server. Scanned events belong to the organization which the user is managing in the program web interface (see page [230](#)) (in the distributed solution and multitenancy mode).
- **Apply to** – name of servers with the Central Node component on which the rule is applied.

The **Query** tab displays the source code of the query being checked. By clicking the link with the text of the query you can navigate to the **Threat Hunting** section and view all events matching the given search criteria (see page [239](#)).

Enabling or disabling an IOA rule

You can enable or disable the use of a single rule or multiple rules, or all rules at the same time.

► *To enable or disable the use of an IOA rule when scanning the events database:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. In the row with the relevant IOA rule, select or clear the check box in the **State** column.
Use of an IOA rule when scanning the events database is enabled or disabled.

► *To enable or disable the use of all or several IOA rules when scanning events:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.

2. Select the check boxes on the left of the rules whose use you want to enable or disable.
You can select all rules by selecting the check box in the line containing the headers of columns.
A control panel appears in the lower part of the window.
3. Click **Enable** or **Disable** to enable or disable all rules.
Use of the selected custom IOA rules when scanning events will be enabled or disabled.

These changes do not affect IOA rules defined by Kaspersky Lab. If you do not want to use a Kaspersky Lab IOA rule for scanning, add it to the white list (see page 331).

Adding an IOA rule

► To add an IOA rule:

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
 2. Click the **Upload** button.
The file selection window opens on your local computer.
 3. Select the file that you want to upload and click the **Open** button.
The **New IOA rule** window opens.
- Click the **Events** link to view a list of threats in the events database matching the criteria defined in the file.
4. Select or clear the **State** check box to apply the rule when scanning the events database.
 5. In the **Name** field, enter the name of the rule.
 6. In the **Description** field, enter any additional information about the rule.
 7. In the **Importance** drop-down list, select the importance level to be assigned to alerts generated using this IOA rule.
 - **Low.**
 - **Medium.**
 - **High.**
 8. In the **Confidence** drop-down list, select the level of confidence of this rule based on your estimate:
 - **Low.**
 - **Medium.**
 - **High.**
 9. Under **Apply to**, select check boxes corresponding to servers on which you want to apply the rule.
 10. On the **Query** tab, verify the defined search conditions. Make changes if necessary.
 11. Click the **Save** button.
The IOA rule is added.

You can also add an IOA rule by saving event database search conditions (see page [265](#)) under **Threat Hunting**.

Editing an IOA rule

You can edit only custom IOA rules. Rules created by Kaspersky Lab cannot be edited.

When working in distributed solution and multitenancy mode, you can edit only those IOA rules that were created on the current server. Consequently, in the web interface of the PCN, you can edit only the rules that were created on the PCN. In the web interface of an SCN, you can edit only the rules that were created on the SCN.

► To edit an IOA rule:

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. Select the IOA rule that you want to edit.
This opens a window containing information about the IOA rule.
3. Make the relevant changes.
4. Click the **Save** button.
The IOA rule settings will be changed.

Deleting an IOA rule

You can delete a single rule or multiple rules, or all rules at the same time.

When working in distributed solution mode, you can delete only those IOA rules that were created on the current server. Consequently, in the web interface of the PCN, you can delete only the rules that were created on the PCN. In the web interface of an SCN, you can delete only the rules that were created on the SCN.

► To delete an IOA rule:

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. Select the IOA rule that you want to delete.
This opens a window containing information about the IOA rule.
3. Click the **Delete** button.
The action confirmation window opens.
4. Click **Yes**.

The IOA rule is deleted.

► *To delete all or several IOA rules:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.

The table of IOA rules opens.

2. Select the check boxes on the left of the rules that you want to delete.

You can select all rules by selecting the check box in the line containing the headers of columns.

A control panel appears in the lower part of the window.

3. Click the **Delete** button.

The action confirmation window opens.

4. Click **Yes**.

The selected custom IOA rules will be deleted.

You cannot delete IOA rules defined by Kaspersky Lab. If you do not want to use a Kaspersky Lab IOA rule for scanning, add it to the white list (see page [331](#)).





Viewing an IOA white list

► *To view the IOA rule white list:*

In the window of the program web interface, select the **IOC/IOA Analysis** section, **IOA White List** subsection.

The white-listed IOA rule table opens. You can filter the rules by clicking links in column headers.

The table of IOA files contains the following information:

1.  The importance level that is assigned to an alert generated using this IOA rule.
The importance level can have one of the following values:
 -  – **Low**.
 -  – **Medium**.
 -  – **High**.
2. **Type** is the type of the rule depending on the role of the server on which it was generated, in distributed solution and multitenancy (see page [43](#)) mode:
 - **Global** – the rule was created on the PCN server.
 - **Local** – the rule was created on an SCN server.
3. **Confidence** – level of confidence depending on the likelihood of false alarms caused by the rule:
 - **High**.
 - **Medium**.
 - **Low**.

The higher the confidence, the lower the likelihood of false alarms.

4. **Name** – name of the rule.
5. **Servers** – name of the server with the Central Node component on which the rule is applied.

Viewing information about an IOA rule in the white list

► *To view information about an IOA rule that was added to the white list:*

1. In the window of the program web interface, select the **IOC/IOA Analysis** section, **IOA White List** subsection.

The white-listed IOA rule table opens.

2. Select the IOA rule whose information you want to view.

This opens a window containing information about the rule.

The window contains the following information:

- **IOA rule.** Click this link to open a window containing a description of the MITRE technique corresponding to this rule, recommendations on responding to the event, and data on the likelihood of false alarms.
- **ID** is the ID that the program assigns to each rule.
- **Name** is the name of the rule that you specified when you added the rule.
- **Importance** is an estimate of the probable impact of the event on the security of computers or the corporate LAN as assessed by Kaspersky Lab experts.
- **Confidence** is the level of confidence depending on the probability of false positives as estimated by Kaspersky Lab experts.
- **Apply to servers*** is a list of organizations and servers on which the IOA rule added to the white list is applied.

Adding an IOA rule to the white list

Only Kaspersky Lab IOA rules can be added to the white list. If you do not want to apply a user-defined IOA rule for scanning the event database, you can disable that rule (see page [327](#)) or delete it (see page [329](#)).

► *To add an IOA rule to the white list from the **Alerts** section:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the link in the **Technologies** column to open the filter configuration window.
3. In the drop-down list on the left, select **Contains**.
4. In the drop-down list on the right, select **(IOA) IOA Analysis**.
5. Click the **Apply** button.

The table displays alerts generated by IOA rules.

6. Select an alert for which the **Detected** column shows the name of the relevant IOA rule.

This opens a window containing information about the alert.

7. Under **Scan results**, click the link with the name of the rule to open the rule information window.
8. Click **Add to white list**.

This opens a window containing information about the rule.

9. Click the **Add** button.

The IOA rule is added to the white list. This rule will be skipped during events database scans.

► *To add an IOA rule to the white list from the **Threat Hunting** section:*

1. Select the **Threat Hunting** section in the program web interface window.

The event search form opens.

2. Define the search conditions and click the **Search** button.

You will see a list of servers on which events meeting the defined criteria were detected.

3. Select the relevant server.

4. Select the event in the table containing the search results.

This opens a window containing information about the event.

5. Click the link in the **IOA tags** field.

This opens a window containing information about the alert.

6. Click **Add to white list**.

This opens a window containing information about the rule.

7. Click the **Add** button.

The IOA rule is added to the white list. This rule will be skipped during events database scans.

Removing an IOA rule from the white list

You can delete a single rule or multiple rules, or all rules at the same time from the white list.

► *To remove an IOA rule from the white list:*

1. In the window of the program web interface, select the **IOC Scanner** section, **IOA White List** subsection.

The table of white-listed IOA rules opens.

2. Select the IOA rule that you want to delete from the white list.

This opens a window containing information about the IOA rule.

3. Click the **Delete** button.

The action confirmation window opens.

4. Click **Yes**.

The IOA rule is removed from the white list. This rule will be applied during events database scans.

► *To delete all or several IOA rules from the white list:*

1. In the window of the program web interface, select the **IOC Scanner** section, **IOA White List** subsection.

The table of white-listed IOA rules opens.

2. Select the check boxes next to the rules that you want to delete from the white list.
You can select all rules by selecting the check box in the line containing the headers of columns.
3. In the pane that appears in the lower part of the window, click **Delete**.
The action confirmation window opens.
4. Click **Yes**.

The selected IOA rules will be deleted from the white list. The rules will be applied when scanning the events database.

Viewing the IOA analysis results

► *To find and view IOA analysis results for user-defined rules:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. Select the IOA rule for which you want to view scan results.
This opens a window containing information about the IOA rule.
3. Do one of the following:
 - If you want to view alerts generated by the IOA rule, click **Alerts** to proceed to the alerts database.
The alert table is opened in a new browser tab.
 - If you want to view events generated by the IOA rule, click **Events** to proceed to the events database.
The event table is opened in a new browser tab.

► *To find and view IOA analysis results for Kaspersky Lab rules:*

1. Select the **Alerts** section in the window of the program web interface.
The table of alerts opens.
2. Click the link in the **Technologies** column to open the filter configuration window.
3. In the drop-down list on the left, select **Contains**.
4. In the drop-down list on the right, select **(IOA) IOA Analysis**.
5. Click the **Apply** button.
The table displays alerts generated by IOA rules.
6. Select an alert for which the **Detected** column shows the name of the relevant IOA rule.
This opens a window containing information about the alert.
7. Under **Scan results**, click the link with the name of the rule to open the rule information window.
8. Do one of the following:
 - If you want to view alerts generated by the IOA rule, click **Alerts** to proceed to the alerts database.
The alert table is opened in a new browser tab.
 - If you want to view events generated by the IOA rule, click **Events** to proceed to the events database.
The event table is opened in a new browser tab.

Filtering and searching IOA rules

► *To filter or search for IOA rules based on required criteria:*


1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. Depending on the filtering criterion, do the following:
 - **By importance**
 - **By rule type**
 - **By confidence level**
 - **By rule name**
 - **By server name**
 - **By rule-based alert generation**
 - **By rule state**

The table of IOA rules displays only IOA rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Clearing an IOA rules filter

► *To clear an IOA rule filter based on one or more filter conditions:*

1. In the program web interface window, select the **IOC/IOA Analysis** section, **IOA Analysis** subsection.
The table of IOA rules opens.
2. Click the  button on the right of the header of the IOC rules table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of IOA rules displays only IOA rules that match the filter criteria you have set.

Managing objects in Backup

You can place copies of objects that you want to scan into special Backup.

Backup is located on the Central Node server.

If you are using the distributed solution and multitenancy mode, Backup is located on PCN and SCN servers. The web-interface of the PCN server displays information about Backup of all connected SCNs for organizations, which the user is allowed to access (see page [160](#)).

Users with the **Senior security officer** role can place copies of objects into Backup using the **Get file** task or by manually uploading the object to Backup (see page [338](#)) on the PCN or SCN server which is used to manage organizations that the user is allowed to access (see page [160](#)).

Users with the **Security officer** role can only work with files received as part of tasks that the same user created on the PCN or SCN server which is used to manage organizations that the user is allowed to access (see page [160](#)).

If you consider an object to be dangerous, you can place it in Quarantine.

Quarantine is a special area of Backup intended for storing files that could potentially cause harm to computers or to the corporate LAN. You can move files from a host to Quarantine so that they can be scanned before they are deleted, or recovered if no threat is present.

When an object is sent to Quarantine, it is moved but not copied: the object is deleted from the host and is saved in Quarantine.

You can manage objects in Backup as follows: delete, download, upload, and send objects to be scanned, and filter lists of objects.

Kaspersky Anti Targeted Attack Platform displays the objects in Backup as a table of objects.

The default maximum size of Backup (in addition to Quarantine) is 10 GB. As soon as this threshold value is exceeded, the program starts to remove the oldest copies of objects from Backup. When the amount of occupied space is again below the threshold value, the program stops removing copies of objects from Backup. Information on Backup space usage is displayed in the **Storage** section, **Capacity** tab.

The maximum size of Quarantine is 10 GB. If the size of Quarantine exceeds the threshold value defined by default, you will not be able to place any new objects into it until you delete some of the old objects. Information about Quarantine space usage is displayed in the **Storage** section, **Capacity** subsection in the upper part of the program web interface window.

The maximum size of a file that can be placed in Quarantine is 100 MB.

The actual file size may be greater than the file apparent size due to metadata required to restore the file from Quarantine. When placed in Quarantine, the file actual size is considered. Encrypted files may be sent in decrypted form (depending on encryption settings), compressed files are sent as-is.




Viewing the table of objects that were placed in Backup

The table of objects placed in Backup is in the **Storage** section, **Files** subsection.

The table of objects placed in Backup contains the following information:

1. **Type**—Location of the object in Backup.

The following types of objects are available:

-  —Object has not been placed in Quarantine.
-  —Object has been placed in Quarantine.
-  —Object was uploaded by the user.

2. **Object**—Information about the object. For example, the file name or file path.

3. **Scan results**—Object scan result.

The scan result is displayed as one of the following values:

- **Not detected**—As a result of a scan, the program did not detect signs of a targeted attack, probably infected objects, or suspicious activity.
- **Error**—Object scan ended with an error.
- **In process**—Object scan has not yet completed.
- **Not scanned**—Object was not sent to be scanned.
- **Detected**—As a result of a scan, the program detected signs of a targeted attack, a probably infected object, or suspicious activity.

4. **Servers**—Name of the Central Node, PCN, or SCN server. The host from which the object was received is connected to this server.
5. **Source**—IP address or name of the host from which the object was received, or the name of the user account that uploaded the object.
6. **Time stored**—Date and time when the object was placed in Backup.

Viewing information about an object in Backup

► *To view information about an object in Backup:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.

The objects table opens.

2. In the table, select the object whose information you want to view.

The object details window opens.

The window contains the following information:

- **File name**—Name of the file.

Clicking the link next to **File name** opens a list in which you can select one of the following actions:

- **Find events.**
- **Find alerts.**
- **Copy value to clipboard.**

- **Size**—Size of the file.
- **MD5**—MD5 hash of a file.

Clicking the link with **MD5** opens a list in which you can select one of the following actions:

- **Find on Kaspersky Threat Intelligence Portal.**
- **Find alerts.**
- **Create a prevention rule.**
- **Copy value to clipboard.**
- **SHA256**—SHA256 hash of a file.
Clicking the link with **SHA256** opens a list in which you can select one of the following actions:
 - **Find on Kaspersky Threat Intelligence Portal.**
 - **Find on virustotal.com.**
 - **Find events.**
 - **Find alerts.**
 - **Create a prevention rule.**
 - **Copy value to clipboard.**
- **Time stored**—Time when the object was placed in Backup.
- **Time uploaded**—Time of upload for objects that were manually uploaded by a user.
- **Company** —Name of the organization to which the Central Node, PCN, or SCN server belongs.
- **Server**—Name of the Central Node, PCN, or SCN server. The host from which the object was received is connected to this server.
- **Host**—Name of the host from which the object was received.
- **User name**—Name of the user account that manually uploaded the object to Backup.
- **Scan results**—Result of object scan by the program.


Downloading objects from Backup

If you consider an object in Backup to be safe, you can download it to a local computer.

Downloading infected objects could pose a threat to the security of your local computer.

► To download an object from Backup:

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.

2. In the right part of the line with the name of the object that you want to download, click 

The object will be saved to your local computer in the browser's downloads folder. The file is downloaded as a ZIP archive protected with the password "infected".

Uploading objects to Backup

If you need to scan a specific object, you can upload this object to Backup and send it to be scanned (see page [338](#)).

► *To upload an object to Backup:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.
2. In the upper-right corner of the window, click the **Upload** button.
The file selection window opens.
3. Select the object that you want to upload to Backup, and click the **Open** button.
The object will be uploaded to Backup and will be displayed in the table of objects.

Scanning objects from Backup

You can scan Backup objects with the Central Node component using the Anti-Malware Engine and YARA technologies, and with the Sandbox component.

It is recommended to send objects from Backup to be scanned in the following cases:

- Scanning of objects when placed in Backup had been disabled.
- Program databases have been updated.
- An object was manually uploaded to Backup.

► *To send an object from Backup to be scanned:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.
2. Click the object that you want to scan.
The object details window opens.
3. Click the **Scan** button.
The object scan will start.
After the object scan is complete, its status will be displayed in the object table.

Deleting objects from Backup

► *To delete an object from Backup:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.
2. Click the object that you want to delete.
The object details window opens.

3. Click the **Delete** button.

The action confirmation window opens.

4. Click **Yes**.

The object will be deleted from Backup.

Filtering objects in Backup by object type

► *To filter objects in Backup by type:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.

The objects table opens.

2. Click the **Type** link to open the object filtering menu.

3. Select one or several check boxes:

- **File in Storage**, if you want the table to display objects that are in Backup but not in Quarantine.
- **Quarantined file**, if you want the table to display objects that have been placed in Quarantine.
- **Uploaded file**, if you want the table to display objects that were manually uploaded by the user.

4. Click the **Apply** button.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering objects in Backup by object description

► *To filter objects in Backup based on the object description:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.

The objects table opens.

2. Click the **Object** link to open the object filtering menu.

3. In the drop-down list, select one of the following options:

- **File path.**
- **MD5.**
- **SHA256.**

4. In the drop-down list, select one of the following object filtering operators:

- **Contains.**
- **Does not contain.**
- **Equal to.**
- **Not equal to.**

- **Matches the pattern**
- **Does not match the pattern**

5. In the entry field, specify one or several characters of the object description.

6. To add a filter condition using a different criterion, click  and specify the filter condition.

7. Click the **Apply** button.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering objects in Backup based on scan results

► *To filter objects in Backup based on the scan results for these objects:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.

The objects table opens.

2. Click the **Scan results** link to open the object filtering menu.

3. Select one or several check boxes:

- **Not detected**
- **Error**
- **In process**
- **Not scanned**
- **Detected**

4. Click the **Apply** button.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering objects in Backup based on the name of Central Node, PCN, or SCN server

► *To filter objects in Backup based on the name of the Central Node, PCN, or SCN server:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.

The objects table opens.

2. Click the **Servers** link to open the object filtering menu.

3. Select one or multiple check boxes opposite those servers by which you want to filter objects in Backup.
4. Click the **Apply** button.


The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering objects in Backup by object source

► *To filter objects in Backup based on the source from which they were received:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.
2. Click the **Source** link to open the object filtering menu.
3. In the drop-down list, select one of the following object filtering operators:
 - **Contains.**
 - **Does not contain.**
4. In the entry field, specify one or several characters of the IP address, host name or name of the user account that manually uploaded the object.

5. To add a filter condition using a different criterion, click  and specify the filter condition.
6. Click the **Apply** button.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering objects based on the time they were placed in Backup

► *To filter objects based on the time they were placed in Backup:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.
2. Click the **Time stored** link to open the object filtering menu.
3. Select one of the following object display periods:
 - **All**, if you want the table to display all objects that were placed in Backup.
 - **Last hour**, if you want the table to display objects that were placed in Backup during the last hour.
 - **Last day**, if you want the table to display objects that were placed in Backup during the last day.


- **Custom range**, if you want the table to display objects that were placed in Backup during the period you specify.
4. If you have selected the **Custom range** object display period:
 - a. In the calendar that opens, specify the start and end dates of the object display period.
 - b. Click the **Apply** button.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

Clearing a Backup objects filter

► *To clear a Backup objects filter based on one or multiple filter conditions:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
The objects table opens.
2. Click the  button on the right of the header of the Backup objects table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The objects table will display only objects matching the filter criteria you have set.

Viewing space usage in Backup and Quarantine

Information on Backup and Quarantine space usage is displayed in the **Storage** section, **Capacity** tab.

The table contains the following information:

1. **Server** is the name of the Central Node, PCN, or SCN server. Hosts that are the source of objects in Backup, connect to this server.
2. **Used space** is the amount of space used in Backup and Quarantine.

The default maximum size of Backup (in addition to Quarantine) is 10 GB. As soon as this threshold value is exceeded, the program starts to remove the oldest copies of objects from Backup. When the amount of occupied space is again below the threshold value, the program stops removing copies of objects from Backup.

The maximum size of Quarantine is 10 GB. If the size of Quarantine exceeds the threshold value defined by default, you will not be able to place any new objects into it until you delete some of the old objects.

Managing reports

When working in the program web interface, users with the **Senior security officer** role can manage reports on program alerts: create report templates (see page [343](#)), create reports based on a template (see page [345](#)), view and delete reports and report templates.

A report is generated based on a selection of alerts for a specified period. If you are using distributed solution and multitenancy mode, data is also selected based on the organization and servers of that organization.

You can manage report templates and reports in all operating modes of the program in accordance with the license.

Perform the report creation steps in the following order:

- a. **Create a report template** (see page [343](#)).
- b. **Create a report based on the template** (see page [345](#)).

Creating a template

When creating a report template, you need to specify all the information that you want to display in the report: report name, its description, availability of a table, graph or image. You can also select the data that you want to display in the report and define the position of report elements.

When creating a report (see page [345](#)) in the **Reports** section, **Generated Reports** subsection of the interface, you can only select the template for creating the report and the data display period.

Create a new report template for each data selection.

► To generate a template:

1. In the program web interface window, select the **Reports** section, **Templates** tab.

The table of templates opens.

2. Click the **Add** button.

The template creation window opens. This window contains the body of the report and the report builder in a floating window. You can move the report builder over the workspace of the web interface window.

3. In the **Report name** field in the upper-right corner of the window, type the name that you want to assign to reports that are created from this template. For example, **Alerts by technology**.

This name is displayed in the table in the **Reports** section, **Generated Reports** subsection when creating all reports in this template.

4. In place of the **Report title** text, type the report name that will be displayed in a report after the report is created. If you do not want to add a report name, you can delete the **Report title** text and leave this report section blank.

You can format text using the buttons in the **Text** section in the template designer.

5. In place of the **Report description** text, type the report description that will be displayed in a report after the report is created. If you do not want to add a report description, you can delete the **Report description** text and leave this report section blank.

You can format text using the buttons in the **Text** section in the template designer.

6. Using the report builder, add one or more report elements:
 - **Table.**
 - **Pie Chart.**
 - **Image.**
 7. If you chose to add an image, the **Image** window opens. Do the following:
 - a. Click the **Upload** button.
 - b. Upload the image. For example, you can upload your company logo.
 - c. In the list on the right of the upload button, select the alignment of the image on the report page: **Left**, **Right** or **Center**.
 - d. Click the **Apply** button.
 8. If you chose to add a pie chart, the **Pie Chart on alert attributes** window opens. Do the following:
 - a. In the **Name** field, type the name of the pie chart. For example, **Top 5 alerts by technology**. You can also leave the field blank.
 - b. In the **Alert attribute** list, select the alert property for which you want to create a pie chart. For example, **Technologies**.
 - c. In the **Number of slices** field, specify the maximum number of sectors of the pie chart. When a report is created, the program selects the most frequently encountered data. For example, if you specified 5 sectors and want to create a pie chart by technology, the program will show a pie chart for the 5 technologies that generated the highest number of alerts. The technologies that generated the lowest number of alerts are not displayed on the pie chart.

Click the **Apply** button.
 9. If you chose to add a table, the **Alerts table** window opens. Do the following:
 - a. In the **Available columns** field, double-click to select the alert properties that you want to add to the report table.

The selected properties are moved to the **Selected columns** field. You can drag the names of columns between the **Available columns** and **Selected columns** fields, and change the order of columns in the report table.

For example, if you moved the **Technologies**, **Detected** and **Time created** properties to the **Selected columns** field, the table of the created report will show the technologies that generated alerts, a list of detected objects, and the time when the alerts were generated.

 - b. If you want to filter alerts by the **State** property, select the check boxes next to the processing statuses of alerts whose data you want to display in the report.
 - c. If you want to filter alerts by the **Technologies** property, select the check boxes next to the names of program modules and components whose data you want to display in the report.
 - d. If you want to filter alerts by the **Importance** property, select the check boxes next to the importance levels of alerts whose data you want to display in the report.
 - e. If you want to filter alerts by the **VIP Status** status, select **VIP** in the list. Only alerts with the VIP status are displayed in the report.
 - f. Click the **Apply** button.
 10. Click the **Save** button in the upper-right corner of the window.
- A new template will be created.

Creating a report based on a template

► *To create a report based on a template:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. Click the **Add** button.
This opens the **New report** window.
3. Do the following:
 - a. In the **Template** drop-down list, select one of the templates for creating a report.
 - b. In the **Period** settings group, select one of the following options:
 - **Last hour**, if you want the report to contain information about program operation during the last hour.
 - **Last day**, if you want the report to contain information about program operation during the last day.
 - **Last 7 days**, if you want the report to contain information about program operation during the last week.
 - **Last 30 days**, if you want the report to contain information about system operation during the last month.
 - **Custom**, if you want the report to contain information about system operation during the period you specify.
4. If you have selected the **Custom** display period for information about program operation:
 - a. In the calendar that opens, specify the start and end dates of the period for which the report will be generated.
 - b. Click the **Apply** button.
5. If you are using distributed solution and multitenancy mode, in the **Servers** settings group select the check boxes next to the organizations and servers whose data you want to display in the report.
6. Click the **Create** button.

The created report is displayed in the table of reports. You can download the report for viewing (see page [346](#)) on your computer.

Viewing the table of templates and reports

Templates and reports are displayed in the **Reports** section of the program web interface window.

The **Generated Reports** subsection contains a report table. The table contains the following information:

- **Time created**—Date and time of report creation.
- **Report name**—Name of the report created based on the template.
- **Servers**—Name of the server with the Central Node component on which the report was created (if you are using distributed solution and multitenancy mode).
- **Period**—Period for which the report was generated.
- **Created by**—Name of the user that created report.

The **Templates** subsection displays the table of templates. The table contains the following information:

- **Time created**—Date and time when the template was created.
- **Time updated**—Date and time of last modification of the template.
- **Report name**—Name of the template.
- **Created by**—Name of the user that created the template.


Viewing a report

► *To view a report:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. Select the report that you want to view.
The report opens in a new tab in your browser.

Downloading a report to a local computer

► *To download a report to your computer:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. In the line containing the report that you want to view, click the  icon.
The report will be saved in HTML format to your local computer in the browser's downloads folder.
To view a report, you can use any application designed for viewing HTML files (for example, a browser).

Editing a template

► *To edit a template:*

1. In the program web interface window, select the **Reports** section, **Templates** tab.
The table of templates opens.
2. Select the template that you want to edit.
The template editing window opens.
3. You can edit the following settings:
 - **Report name** – report name that is displayed in the table in the **Reports** section, **Generated Reports** subsection when creating all reports based on this template.
 - **Report title** – report name that is displayed in a report after the report is created.
You can format text using the buttons in the **Text** section in the template designer.
 - **Report description** – report description that is displayed in a report after it is created.

You can format text using the buttons in the **Text** section in the template designer.

- **Image.** You can upload or delete an image.
- **Pie Chart.** You can change the following pie chart settings:
 - **Name.**
 - **Alert attribute.**
 - **Number of slices.**

Click the **Apply** button.


- **Table.** You can change the following table settings:
 - **Selected columns.** You can drag the names of columns between the **Available columns** and **Selected columns** fields, and change the order of columns in the report table.
 - **State.**
 - **Technologies.**
 - **Importance.**
 - **VIP Status.**
4. Select one of the following methods to save the template:
- If you want to apply changes to the current template, click the **Save** button.
The template will be changed.
 - If you want to create a new template, enter a name for it and click the **Save as** button.

The name of the new template must not be the same as the name of an already existing template.

The new template will be saved.

Filtering templates by name

► To filter templates by name:

1. In the program web interface window, select the **Reports** section, **Templates** tab.
The table of templates opens.
2. Click the **Report name** link to open the template filtering menu.
3. In the drop-down list, select one of the following template filtering operators:
 - **Contains.**
 - **Does not contain.**
4. Enter one or several characters of the template name.
5. If you want to add a filtering criterion to the filter, click the  button under the list of filtering operators and repeat the sequence for specifying filtering criteria.
6. Click the **Apply** button.

The table of templates will display only templates that match the filter criteria you have set.

Filtering templates based on the name of the user that created the template

► *To filter templates by the name of the user that created the template:*


1. In the program web interface window, select the **Reports** section, **Templates** tab.

The table of templates opens.

2. Click the **Created by** link to open the menu for filtering templates.
3. In the drop-down list, select one of the following template filtering operators:

- **Contains.**
- **Does not contain.**

4. Enter one or several characters of the user name.

5. If you want to add a filtering criterion to the filter, click the  button under the list of filtering operators and repeat the sequence for specifying filtering criteria.

6. Click the **Apply** button.

The table of templates will display only templates that match the filter criteria you have set.

Filtering templates by creation time

► *To filter report templates based on the time when they were created:*

1. In the program web interface window, select the **Reports** section, **Templates** tab.

The table of templates opens.

2. Click the **Time created** link to open the menu for filtering templates.

3. Select one of the following template display periods:

- **All**, if you want the program to display all created templates in the table.
- **Last hour**, if you want the program to display the templates that were created during the last hour in the table.
- **Last day**, if you want the program to display the templates that were created during the last day in the table.
- **Custom range**, if you want the program to display templates that were created during the period you specify in the table.

4. If you have selected the **Custom range** template display period:

- a. In the calendar that opens, specify the start and end dates of the template display period.
- b. Click the **Apply** button.


The table of templates will display only templates that match the filter criteria you have set.

Clearing a template filter

► *To clear a template filter based on one or multiple filter conditions:*

1. In the program web interface window, select the **Reports** section, **Templates** tab.

The table of templates opens.

2. Click the  button on the right of the header of the templates table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of templates will display only templates that match the filter criteria you have set.

Deleting a template

► *To remove a template:*

1. In the program web interface window, select the **Reports** section, **Templates** tab.

The table of templates opens.

2. Select the check box in the line containing the template that you want to delete.
3. Click the **Delete** button.

The action confirmation window opens.

4. Click **Yes**.

The template that you selected will be deleted.

Filtering reports by creation time

► *To filter reports based on their creation time:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.

The table of reports opens.

2. Click the **Time created** link to open the report filtering menu.

3. Select one of the following report display periods:


- **All**, if you want the program to display all created reports in the table.
- **Last hour**, if you want the program to display the reports that were created during the last hour in the table.
- **Last day**, if you want the program to display the reports that were created during the last day in the table.

- **Custom range**, if you want the program to display reports that were created during the period you specify in the table.
4. If you have selected the **Custom range** report display period:
 - a. In the calendar that opens, specify the start and end dates of the report display period.
 - b. Click the **Apply** button.

The table of reports will display only reports that match the filter criteria you have set.

Filtering reports by name

► *To filter reports by name:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. Click the **Report name** link to open the report filtering menu.
3. In the drop-down list, select one of the following report filtering operators:
 - **Contains.**
 - **Does not contain.**
4. In the entry field, specify one or several characters of the report name.
5. If you want to add a filtering criterion to the filter, click the  button under the list of filtering operators and repeat the sequence for specifying filtering criteria.
6. Click the **Apply** button.

The table of reports will display only reports that match the filter criteria you have set.

Filtering reports by the name of the server with the Central Node component

► *To filter reports based on the name of the server with the Central Node component:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. Click the **Servers** link to open the report filtering menu.
3. Select the check boxes opposite those servers by which you want to filter reports.
4. Click the **Apply** button.


The table of reports will display only reports that match the filter criteria you have set.

Filtering reports based on the name of the user that created the report

► *To filter reports based on the name of the user that generated the report:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.


The table of reports opens.

2. Click the **Created by** link to open the report filtering menu.
3. In the drop-down list, select one of the following report filtering operators:
 - **Contains.**
 - **Does not contain.**
4. Enter one or several characters of the user name.
5. If you want to add a filtering criterion to the filter, click the  button under the list of filtering operators and repeat the sequence for specifying filtering criteria.

The table of reports will display only reports that match the filter criteria you have set.

Clearing a report filter

► *To clear a report filter based on one or multiple filter conditions:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. Click the  button on the right of the header of the reports table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of reports will display only reports that match the filter criteria you have set.

Deleting a report

► *To delete a program operation report:*

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.
The table of reports opens.
2. Select the check box in the line containing the report that you want to delete.
3. Click the **Delete** button.
The action confirmation window opens.
4. Click **Yes**.

The selected report will be deleted.

Sending notifications




You can configure forwarding of notifications to one or multiple email addresses.

The program can provide notifications about alerts and about program operation problems.

Viewing the table of rules for sending notifications

Rules for sending notifications are displayed in the **Settings** section, **Notifications** subsection of the program web interface window.

The table of rules for sending notifications contains the following information:

-  —Type of rule for sending notifications.
The following types of rules are possible:
 -  —Rule for sending a notification about alerts.
 -  —Rule for sending a notification about the operation of program components.
- **Subject**—Subject of the message containing the notification.
- **To**—Email addresses to which the notifications are sent.
- **State**—Status of the rule for sending a notification.

Creating a rule for sending notifications about alerts

► *To create a rule for sending notifications about alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the **Add** button.
The **New notification rule** window opens.
3. In the **To** field, specify one or several email addresses to which you want to forward notifications.
You can enter several email addresses if you separate them with commas.
4. In the **Subject** field, specify the subject of the message containing the notification.
5. If you want the program to insert the alert importance into the message subject, add the `%importance%` macro into the **Subject** field.
6. In the **Notification type** field, select **Alerts**.
7. In the **Alert importance** drop-down list, select the minimum alert importance for which you want to configure notifications to be sent regarding such alerts.
For example, you can configure forwarding of notifications for only alerts that have high importance, or for only those that have medium or high importance.
8. In the **Source or destination** field, specify an IP address and network mask if you want to configure forwarding of notifications about alerts associated with a specific IP address or subnet address of the source or destination.

9. In the **Email** field, specify an email address if you want to configure forwarding of notifications about alerts associated with a specific address of the sender or recipient of email messages.
10. In the **Components** settings group, select the check boxes next to the names of one or several technologies if you want to configure forwarding of notifications about alerts generated by specific technologies.
11. Click the **Add** button.

The rule for sending notifications about alerts will be added to the list of rules.

Creating a rule for sending notifications about the operation of program components

► *To create a rule for sending notifications about the operation of program components:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the **Add** button.
The **New notification rule** window opens.
3. In the **To** field, specify one or several email addresses to which you want to forward notifications.
You can enter several email addresses if you separate them with commas.
4. In the **Subject** field, specify the subject of the message containing the notification.
5. If you want the program to insert the alert importance into the message subject, add the `%importance%` macro into the **Subject** field.
6. In the **Notification type** field, select **Program operation**.
7. In the **Components** settings group, select the check boxes next to the names of the program's functional scopes for which you want to receive notifications.
8. Click the **Add** button.

The rule for sending notifications about the operation of program components will be added to the list of rules.

Enabling and disabling a rule for sending notifications

► *To enable or disable a rule for sending notifications about alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. In the line containing the rule for sending notifications that you want to enable or disable, in the **State** column perform one of the following actions:
 - Turn on the toggle switch if you want to enable the rule.
 - Turn off the toggle switch if you want to disable the rule.

The state of the rule for sending notifications about alerts will be modified.

Modifying a rule for sending notifications

► *To modify a rule for sending notifications:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. In the list of rules for sending notifications, select the rule that you want to modify.
The **Edit notification rule** window opens.
3. Make the relevant changes.
4. Click the **Save** button.

The rule for sending notifications will be modified.

Deleting a rule for sending notifications


► *To delete a rule for sending notifications:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Select the check box to the left of the name of each rule that you want to delete.
If you want to delete all rules, select the check box above the list.
3. Click **Delete** in the lower part of the window.
4. In the confirmation window, click **Yes**.

The selected rules will be deleted.

Filtering and searching notification forwarding rules by rule type

► *To filter or search for notification forwarding rules based on the rule type:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the  icon in the table of rules for sending notifications.
The filter configuration window opens.
3. Select one of the following options:
 - **All**
 - **Alerts.**
 - **Program operation.**

The table of notification forwarding rules will display only rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering and searching notification forwarding rules based on the notification subject

► *To filter or search for notification forwarding rules based on the notification subject:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the **Subject** link to open the filter configuration window.
3. Enter one or several characters of the notification subject.
4. Click the **Apply** button.

The filter configuration window closes.

The table of notification forwarding rules will display only rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering and searching notification forwarding rules by email address

► *To filter or search for notification forwarding rules based on their destination email address:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the **To** link to open the filter configuration window.
3. Enter one or several characters of the email address.
4. Click the **Apply** button.

The table of notification forwarding rules will display only rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering and searching notification forwarding rules based on their status

► *To filter or search for notification forwarding rules based on their status:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the **State** link to open the filter configuration window.
3. Select one or several check boxes next to the values of statuses:
 - **Enabled**
 - **Disabled**
4. Click the **Apply** button.


The filter configuration window closes.

The table of notification forwarding rules will display only rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Clearing a notification forwarding rule filter

► *To clear a notification forwarding rules filter based on one or multiple filter conditions:*

1. In the main window of the program web interface, select the **Settings** tab, **Notifications** section.
2. Click the  button on the right of the header of the notification forwarding rules table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table of notification forwarding rules will display only rules that match the filter criteria you have set.

Managing rules for assigning the VIP status to alerts

You can create, import, or export a list of rules for assigning the VIP status to alerts. Alerts with the VIP status are available only to users with the **Senior security officer** role.

You can create the following types of rules:

- **IP.** The VIP status will be assigned to new alerts associated with this IP address of the computer.
- **Host name.** The VIP status will be assigned to new alerts associated with this host name.
- **Email.** The VIP status will be assigned to new alerts associated with this email address.

Adding a VIP status assignment rule

► *To add a rule for assigning the VIP status to alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. In the upper-right corner of the program web interface window, click the **Add** button.

The window for adding a rule opens.

3. In the **Rule type** drop-down list, select one of the following rule types:

- **IP**, if you want to add a rule for a computer IP address.
- **Host name**, if you want to add a rule for a host name.
- **Email**, if you want to add a rule for an email address.

4. Enter the necessary value in the **Value** field.

For example, if under **Rule type**, you selected **Email**, enter the email address that you want to add in the **Value** field.

5. In the **Description** field, enter additional information if necessary.
6. Click the **Add** button.

The rule is added. The VIP status will be assigned to new alerts associated with the added IP address, host name, or email address.

Deleting a VIP status assignment rule

► *To remove a rule for assigning the VIP status to alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Select the check box to the left of each rule that you want to remove from the list.
3. If you want to delete all rules, select the check box above the list.
4. In the upper-right corner of the program web interface window, click the **Delete** button.

The action confirmation window is displayed.

5. Click **Yes**.

The selected rules will be deleted.

Modifying a VIP status assignment rule

► *To modify a rule for assigning the VIP status to alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Select the rule that you want to modify.
The rule editing window opens.
3. Make the necessary changes to the **Rule type**, **Value** and **Description** fields.
4. Click the **Save** button.

The rule is modified.

Importing a list of VIP status assignment rules

► *To import a list of rules for assigning the VIP status to alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Click the **Import** button.

You will be prompted for confirmation of the list import.

The imported list of rules for assigning the VIP status to alerts will replace the current list of VIP status alert assignment rules.

3. Click **Yes**.

The file selection window opens.

4. Select a JSON file containing the list of rules that you want to import and click **Open**.

The file selection window closes.

The list will be imported.

Exporting a list of VIP status assignment rules

► *To export a list of rules for assigning the VIP status to alerts:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. In the upper-right corner of the program web interface window, click the **Export** button.

The list of VIP status assignment rules is exported to a JSON file.

Filtering and searching by type of VIP status assignment rule

► *To filter or search for VIP status assignment rules by rule type:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Click the **Rule type** link to open the filter configuration window.
3. Select one or several check boxes next to the types of rules:
 - **IP.**
 - **Host name.**
 - **Email.**
4. Click the **Apply** button.

The filter configuration window closes.

The table will display only the rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering and searching by value of VIP status assignment rule

► *To filter or search for VIP status assignment rules by rule value:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Click the **Value** link to open the filter configuration window.
3. Enter one or several characters of the rule value.
4. Click the **Apply** button.

The filter configuration window closes.

The table will display only the rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Filtering and searching by description of VIP status assignment rule

► *To filter or search for VIP status assignment rules by description:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Click the **Description** link to open the filter configuration window.
3. Enter one or several characters of the description.
4. Click the **Apply** button.


The filter configuration window closes.

The table will display only the rules that match the filter criteria you have set.

You can use multiple filters at the same time.

Clearing a VIP status assignment rule filter

► *To clear a VIP status assignment rules filter based on one or multiple filter conditions:*

1. In the main window of the program web interface, select the **Settings** tab, **VIP Status** section.
2. Click the  button on the right of the header of the table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The table will display only the rules that match the filter criteria you have set.

Managing YARA rules

YARA rule files are used as the YARA module's databases.

You can create your own YARA rules and add a YARA rule file to Kaspersky Anti Targeted Attack Platform through the program web interface.

For more information about creating and updating YARA rules of version 3.7.0 and higher, please refer to the documentation on YARA rules or visit the website

<http://yara.rules.com/http://yara.rules.com/http://yara.rules.com/http://yara.rules.com/>.

Uploading YARA rules

► *To upload YARA rules:*

1. In the window of the program web interface, select the **Settings** section, **YARA Rules** subsection.
2. Click the **Upload** button.

The file selection window opens.

3. Select the YARA rules file that you want to upload and click the **Open** button.

The file selection window closes.

You will see the following information about the uploaded YARA rules:

- **File size**—Size of the YARA rules file.
- **Time uploaded**—Date and time when a YARA rules file was last uploaded.

Updating YARA rules

► *To update YARA rules:*

1. In the window of the program web interface, select the **Settings** section, **YARA Rules** subsection.
2. Click the **Replace** button.
The file selection window opens.
3. Select the YARA rules file that you want to use to replace the current file and click the **Open** button.
The file selection window closes.
The loaded YARA rules file will replace the previous file.

Deleting YARA rules

► *To delete YARA rules:*

1. In the window of the program web interface, select the **Settings** section, **YARA Rules** subsection.
2. Click the **Delete** button.
The action confirmation window opens.
3. Click **Yes**.
The YARA rules will be deleted.

Managing a white list

You can create, import or export a *white list*, which is a list of data that Kaspersky Anti Targeted Attack Platform will treat as safe and will not display in the alerts table (see page [236](#)). You can add the following data to the white list:

- **MD5**
- **Format**
- **URL mask**
- **Email**
- **Subnet mask**
- **User Agent**

Adding a record to the white list

► *To add a record to the white list:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. In the upper-right corner of the program web interface window, click the **Add** button.
The **New rule** window opens.
3. In the **Rule type** drop-down list, select one of the following criteria for adding a record to the white list:
 - **MD5**
 - **Format**
 - **URL mask**
 - **Email**
 - **Subnet mask**
 - **User Agent**
4. If you selected **Format**, select the file format that you want to add from the **Value** drop-down list.
For example, you can select the **MSOfficeDoc** format.
5. If you selected **MD5**, **URL mask**, **Email**, **User Agent** or **Subnet mask**, enter the value of the relevant criterion that you want to add to the white list in the **Value** field.
 - If you selected **MD5**, enter the MD5 hash of the file in the **Value** field.
 - If you selected **URL mask**, enter the URL mask in the **Value** field.

You can use the following special characters in the mask:

* – any sequence of characters.

Example:

If you enter `*abc*` as the mask, the program considers as safe any URL that contains the sequence `abc`.
For example, `www.example.com/download_virusabc`

? – any single character.

Example:

If you enter `example_123?.com` as the mask, the program considers as safe any URL that contains the given character sequence and any character following 3. For example, `example_1234.com`

If the `*` or `?` characters are part of the full URL that you want to add to the white list, use the `\` character when entering the URL to cancel a single `*`, `?` or `\` character that follows it.

Example:

You need to add the following URL as a trusted address:

`www.example.com/download_virus/virus.dll?virus_name=`

You do not want the program to treat `?` as a special mask character so you put a `\` character before the `?` character.

The URL added to the white list looks as follows:

`www.example.com/download_virus/virus.dll\?virus_name=`

- If you selected **Email**, enter the email address in the **Value** field.
- If you selected **User Agent**, enter the User agent header of HTTP requests containing browser information in the **Value** field.
- If you selected **Subnet mask**, enter the subnet mask in the **Value** field. For example, 255.255.255.0

In the **URL mask** and **Email** field, you can enter domain names containing Cyrillic characters. In this case, the address is converted to Punycode and processed in accordance with program settings.

6. Click the **Add** button.

The record will be added to the white list.

Removing a record from the white list

► *To remove one or multiple records from the white list:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. Select the check box to the left of each record that you want to remove from the white list.

If you want to delete all records, select the check box above the list.

3. In the upper-right corner of the window, click the **Delete** button.

The action confirmation window is displayed.

4. Click **Yes**.

The selected records will be removed from the white list.

Modifying a record in the white list

► *To modify a record in the white list:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. Select the record that you want to modify.
This opens the **Change notification** window.
3. Make the necessary changes to the **Rule type** and **Value** fields.
4. Click the **Save** button.
The record will be modified.

Importing a white list

The imported white list will replace the current white list.

► *To import a white list:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. In the upper-right corner of the program web interface window, click the **Import** button.
The action confirmation window is displayed.
3. Click **Yes**.
The file selection window opens.
4. Select a JSON file containing the white list that you want to download and click the **Open** button.
The file selection window closes.
The white list will be imported. The imported white list will replace the current white list.

Exporting a white list

► *To export a white list:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. In the upper-right corner of the program web interface window, click the **Export** button.

The JSON file containing the exported white list will be saved in the browser's downloads folder on your computer.

Filtering and searching records in the white list based on the type of rule

► *To filter or search for white list records based on the type of rule:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. Click the **Rule type** link to open the filter configuration window.
3. Select one or more check boxes next to rule types by which you want to filter records:
 - **MD5.**
 - **Format**
 - **URL mask**
 - **Email.**
 - **Subnet mask.**
 - **User Agent.**
4. Click the **Apply** button.

The filter configuration window closes.

The white list will display only records matching the filter criteria you have set.

You can use multiple filters at the same time.

Filtering and searching records in the white list based on a value of rules

► *To filter or search for white list records based on a value of rules:*


1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. Click the **Value** link to open the filter configuration window.
3. Enter one or several characters of the value.
4. Click the **Apply** button.

The white list will display only records matching the filter criteria you have set.

You can use multiple filters at the same time.

Clearing a white list record filter

► *To clear a white list records filter based on one or multiple filter conditions:*

1. In the main window of the program web interface, select the **Settings** tab, **White List** section.
2. Click the  button on the right of the header of the white list records table column for which you want to clear the filter conditions.

If you want to clear several filter conditions, perform the necessary actions to clear each filter condition.

The selected filters are cleared.

The white list will display only records matching the filter criteria you have set.

Creating a list of passwords for archives

The program does not scan password-protected archives. You can create a list of the most frequently encountered passwords for archives that are used when exchanging files within your organization. If you do so, the program will try the passwords from the list when scanning an archive. If one of the passwords match, the archive will be unlocked and scanned.

The list of passwords defined in the program settings is also transmitted to the server with the Sandbox component.

► *To create a list of passwords for archives:*

1. In the window of the program web interface, select the **Settings** section, **Passwords to archives** subsection.
2. In the **Passwords to archives** field, enter the passwords that the program will use for password-protected archives.

Enter each password on a new line. You can enter up to 50 passwords.

3. Click the **Apply** button.

The list of passwords for archives will be created. When scanning PDF files and files of Microsoft Word, Excel, and PowerPoint that are password protected, the program will use the passwords from the defined list.

Creating a backup copy and restoring the program from backup

You can create a backup copy of Kaspersky Anti Targeted Attack Platform and subsequently restore the program from the backup copy.

If you are not using the distributed solution and multitenancy mode and are using a standalone Central Node server, you can create a backup copy of the data of that Central Node server.

If you are using distributed solution and multitenancy mode, you can:

1. Create a backup copy of PCN data.
2. Create a backup copy of SCN data. Restoring data from a backup copy of the SCN will change the role of the server from SCN to standalone Central Node server.

Follow the procedure for creating the backup copy of the program on the server for which you want to create a backup copy of the data.

Kaspersky Anti Targeted Attack Platform may contain user data and other confidential information. The Kaspersky Anti Targeted Attack Platform administrator must independently ensure the security of this data when creating a backup copy of the program, when replacing equipment on which the program is installed, or in other cases when it may be necessary to permanently delete data. The Kaspersky Anti Targeted Attack Platform administrator bears responsibility for access to data stored on program servers.

You can create a backup copy of the following data:

- Program databases (alerts database, tasks, policies, information about alert VIP status, white lists, notifications).
- Quarantine.
- Database of alerts generated during a rescan.
- Sandbox artifacts.
- Central Node or PCN settings:
 - If you are using a standalone Central Node server, a backup copy of Central Node settings is created.
 - If you are using the distributed solution and multitenancy mode and are managing the PCN server, a backup copy of PCN settings is created.
 - If you are using the distributed solution and multitenancy mode and are managing the SCN server, you can create a backup copy of the SCN, but restoring data from a backup copy will change the role of the server from SCN to standalone Central Node server.

You can clear the directory before creating a backup copy of the program.

Before the program is restored from a backup copy, the following is cleared on the Central Node or PCN server on which the program is being restored:

- Program databases (alerts database, tasks, policies, information about alert VIP status, white lists, notifications).

- Quarantine.
- Database of alerts generated during a rescan.
- Sandbox artifacts.
- Central Node or PCN settings.

Table 18. Contents and volume of data exported for the creation of a backup copy of the program

Maximum data volume	Data type	Exported data	Program operation mode
4 GB	Central Node settings Program databases on the Central Node (alerts database, tasks, policies, information about alert VIP status, white lists, notifications).	Central Node settings, if selected. Program databases, by default.	Standalone Central Node server.
4 GB	PCN settings.	Custom	Distributed solution and multitenancy mode.
4 GB	PCN settings.	Custom As for a standalone Central Node server.	Distributed solution and multitenancy mode.
4 GB	Program databases on the PCN (alerts database, tasks, policies, information about alert VIP status, white lists, notifications).	Default	Distributed solution and multitenancy mode.
300 GB	Quarantine.	Custom	All modes.
300 GB	Sandbox artifacts.	Custom	All modes.
300 GB	Database of alerts generated during a rescan.	Custom	All modes.
None	Targeted Attack Analyzer database.	By default (HBase data).	All modes.
None	Events database.	None.	All modes.

Files that are in the scan queue when the backup copy of the program is created are not exported.

Creating a backup copy of the program from the program administrator menu

► *To create a backup copy of Kaspersky Anti Targeted Attack Platform, in the administrator menu of the server: (see page [154](#))*

1. In the list of sections of the program administrator menu, select the **System administration** section.
2. Press **ENTER**.
The action selection window opens.
3. In the list of actions, select **Backup/Restore settings**.
4. Press **ENTER**.
The **Backup/Restore settings** window opens.
5. In the list of actions, select **New**.
6. Press **ENTER**.
The **Backup settings** window opens.
7. Click the **Back up** button.

A backup copy of Kaspersky Anti Targeted Attack Platform is created on the server.

Downloading a file containing a backup copy of the program from the Central Node or PCN server to the hard drive of the computer

It is recommended to save files containing a backup copy of the program to the hard drive of your computer.

► *To download a file containing a backup copy of the program to the hard drive of your computer, run the following command in the command line interface of the Linux operating system on your computer:*

```
scp <name of the account used for working in the administrator menu and in the server management console>@<IP address of the server>:<name of the file containing the backup copy of the program in the form of settings-
<date and time of backup copy creation>.tar.gz>
```

Example:

Command for downloading to the hard drive of your computer an archive containing a backup copy of the program that was created on a Central Node server with the IP address 10.0.0.10 under the admin account on April 10, 2019 at 10 hours 00 minutes 00 seconds:

```
scp admin@10.0.0.10:settings-20190410-100000.tar.gz
```

The file containing a backup copy of the program will be saved to the hard drive of your computer in the current folder.

Uploading a file containing a backup copy of the program from your computer to the Central Node server

- To download a file containing a backup copy of the program from the hard drive of your computer to the server, run the following command in Technical Support Mode:

```
scp <name of the file containing a backup copy of the program in the form of settings-<backup copy creation date and time>.tar.gz> <name of the account used for working in the administrator menu and in the server management console>@<IP address of the server>:
```

Example:

Command for uploading an archive containing a backup copy of the program created on April 10, 2019 at 10 hours 00 minutes 00 seconds to the Central Node server with the IP address 10.0.0.10 under the admin account:

```
scp settings-20190410-100000.tar.gz admin@10.0.0.10:
```

The file containing the backup copy of the program will be uploaded to the Central Node server in the current folder.

Restoring the program from a backup copy through the program administrator menu

To restore Kaspersky Anti Targeted Attack Platform from a backup copy, you must first create a backup copy of the current state of the program (see page [369](#)) and download it to the hard drive of your computer. If an error occurs when restoring the program or if it becomes necessary to reinstall Kaspersky Anti Targeted Attack Platform, you will be able to use the saved copy of the program.

- To restore Kaspersky Anti Targeted Attack Platform from a previously created backup copy, perform the following actions in the administrator menu (see page [154](#)) of the server:
1. In the list of sections of the program administrator menu, select the **System administration** section.
 2. Press **ENTER**.
The action selection window opens.
 3. In the list of actions, select **Backup/Restore settings**.
 4. Press **ENTER**.
The **Backup/Restore settings** window opens.
 5. In the list of files containing backup copies of the program, select the file from which you want to restore the program.
If the necessary file is not on the list, download the file containing the backup copy of the program to the server.

6. Press **ENTER**.

The action selection window opens.

7. In the list of actions, select **Restore** <name of the file with the backup copy of the program>.

8. Press **ENTER**.

The action confirmation window opens.

9. Click the **Restore** button.

Kaspersky Anti Targeted Attack Platform will be restored from the file containing the backup copy of the program.

Creating a backup copy of the program in Technical Support Mode

- To create a backup copy of Kaspersky Anti Targeted Attack Platform, run the following command in Technical Support Mode (see page [155](#)) of the server:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh
```

You can also specify one or multiple parameters for this command (see the table below).

You can use the `-h` command to receive tips on using parameters.

Table 19. Parameters of the command for creating a backup copy of Kaspersky Anti Targeted Attack Platform

Required parameter	Parameter	Description
Yes	<code>-b <path></code>	Create a file containing a backup copy of the program at the specified path, where <path> is the absolute path or relative path to the folder in which the file with the backup copy of the program is created.
None	<code>-q</code>	Save files in Quarantine.
None	<code>-a</code>	Save files awaiting rescan.
None	<code>-s</code>	Save Sandbox artifacts.
None	<code>-n</code>	Save Central Node or PCN settings.
None	<code>-l <filepath></code>	Save the command execution result to a file, where <filepath> is the name of the event log file, including the absolute path or relative path to the file.

If additional settings are not defined, the backup copy of Kaspersky Anti Targeted Attack Platform contains only databases (alerts database, VIP status details, white lists, notifications).

All files containing a backup copy of the program are saved to one TAR archive. Archive file name: data_kata_ddmmyyyhhMM, where ddmmyyyy is the date and hhMM is the hour and minute when the backup copy of the program was created. The name of the database is KATA3.6.sql for the backup copy of the program version 3.6.

Example:

Command for creating a backup copy of the program with all parameters:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh -b <path> -q -a -s -n -l <filepath>
```

Restoring the program from a backup copy in Technical Support Mode

- To restore Kaspersky Anti Targeted Attack Platform from a backup copy, run the following command in Technical Support Mode (see page [155](#)) of the server:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh
```

You can also specify one or multiple parameters for this command (see the table below).

You can use the `-h` command to receive tips on using parameters.

Table 20. Parameters of the command for restoring Kaspersky Anti Targeted Attack Platform from a backup copy

Required parameter	Parameter	Command description
Yes	<code>-r <path></code>	Restore data from a file containing a backup copy of the program, where <code><path></code> is the absolute path or relative path to the folder containing the file
None	<code>-c <path></code>	Prior to starting restoration of the program, clear the folder at the specified path, where <code><path></code> is the absolute path or relative path to the folder in which the program upgrade file is created. After this command is executed, the program also checks for free disk space.
None	<code>-l <filepath></code>	Save the command execution result to a file, where <code><filepath></code> is the name of the event log file, including the absolute path or relative path to the file.

Example:

Command for restoring the program from a backup copy with all parameters:

```
/opt/kaspersky/apt-base/bin/ie_kata.sh -r <path> -c <path> -l <filepath>
```

Upgrading Kaspersky Anti Targeted Attack Platform

You can upgrade Kaspersky Anti Targeted Attack Platform from version 3.5 to version 3.6.

You can also install the program update packages released by Kaspersky Lab.

If you are not using the distributed solution and multitenancy mode and are using a standalone Central Node server, you can update the program on the Central Node server.

If you are using the distributed solution and multitenancy mode:

1. You can update the program on the PCN server. After the program update is complete, the PCN server belongs to the same organization it belonged to before the update.
2. If you want to update the program on an SCN server, change the role of the server from SCN to standalone Central Node server before performing the update.

The program is updated on the standalone Central Node server.

After updating the program, you can assign the SCN role to servers and select the organization to which the SCN server belongs (see page [50](#)).

3. After the program update is complete, by default, all users with the Administrator role are granted access to the web interface of the PCN server and all SCN servers.

If before the program update, each user's access to SCN web interfaces was configured individually, you can configure it again (see page [160](#)).

After the program update is complete, by default, all users with the Senior security officer and Security officer roles are granted access to the web interface of the PCN server and all SCN servers.

If before the program update, each user's access to SCN web interfaces was configured individually, you can configure it again (see page [160](#)). To do so, in the web interface of the PCN server:

1. Add the relevant organizations. (see page [52](#))
2. Configure the access of user accounts with the Senior security officer and Security officer roles to these organizations and servers. (see page [160](#))
3. Delete all SCNs that are temporarily disconnected from the PCN during the update (see page [53](#)).
4. Re-connect all relevant SCNs to the PCN (see page [50](#)).

The program prompts you to select an organization for each SCN server.

User access to SCN web interfaces is configured.

Perform the program update procedure on the server where you want to update the data.

Kaspersky Anti Targeted Attack Platform may contain user data and other confidential information. The Kaspersky Anti Targeted Attack Platform administrator must independently ensure the security of this data when upgrading the program, or in other cases when it may be necessary to permanently delete data. The Kaspersky Anti Targeted Attack Platform administrator bears responsibility for access to data stored on program servers.

Table 21. Contents and volume of data saved when upgrading the program from version 3.5 to version 3.6

Maximum data volume	Data type	Data saved during upgrade
4 GB	Central Node settings. Program databases on the Central Node (alerts database, tasks, policies, information about alert VIP status, white lists, notifications).	All data except: <ul style="list-style-type: none"> • Settings for integration with sensors • Keys • Layouts in the Dashboard section
4 GB	PCN settings.	All data except: <ul style="list-style-type: none"> • Settings for integration with sensors • Keys • Layouts in the Dashboard section
4 GB	Program databases on the PCN (alerts database, tasks, policies, information about alert VIP status, white lists, notifications).	All data.
300 GB	Quarantine.	All data.
300 GB	Sandbox artifacts.	All data.
300 GB	Database of alerts generated during a rescan.	All data.
None	Targeted Attack Analyzer database.	All data.
None	Events database.	None.

Files that are in the scan queue when Kaspersky Anti Targeted Attack Platform is upgraded to version 3.6 are not saved.

Upgrading the program from version 3.5 to version 3.6

Prior to upgrading the program from version 3.5 to version 3.6, it is recommended to first create a backup copy of the current state of the program (see page [369](#)) and download it to the hard drive of your computer from the program administrator menu. If an error occurs when upgrading the program or if it becomes necessary to reinstall Kaspersky Anti Targeted Attack Platform, you will be able to use the saved copy of the program.

► *To upgrade the program from version 3.5 to version 3.6, perform the following actions on the Central Node server:*

1. Run the disk image containing the Central Node and Sensor components of Kaspersky Anti Targeted Attack Platform version 3.6. The disk image is included in the program distribution kit (see page [21](#)).

The Setup Wizard starts.

2. Select installation from the **Kaspersky Anti Targeted Attack Platform** installation disk.

The program installation start window opens.

3. Click **OK**.

You will see a window in which you can select the language for viewing the End User License Agreement and Privacy Policy.

To continue installation, you need to read the End User License Agreement and Privacy Policy and accept their terms. Installation will not continue until you accept the terms of the End User License Agreement and Privacy Policy.

4. Select the language for viewing the End User License Agreement and Privacy Policy in the list.

For example, if you want to view the End User License Agreement and Privacy Policy in English, select English.

5. Press **ENTER**.

This opens a window showing the End User License Agreement text.

6. Please read the End User License Agreement.

7. If you accept the terms of the End User License Agreement, click the **I accept the terms** button.

This opens a window displaying the text of the Privacy Policy.

8. Please carefully read the Privacy Policy.

9. If you accept the terms of the Privacy Policy, click the **I accept the terms** button.

The **Select device** window opens.

10. In the **Select device** window, in the list of disks, select the disk where version 3.5 of the program is installed.

11. Press **ENTER**.

The **Select action** window opens.

12. In the list of actions, select **Upgrade**.

13. Press **ENTER**.

You will see a window warning you that version 3.5 of the program is already installed on the drive and that you can upgrade the program to a new version.

14. Click the **Upgrade** button.

Kaspersky Anti Targeted Attack Platform version 3.6 will be installed on the Central Node server. The server is restarted. The program settings available for upgrading the program from version 3.5 to version 3.6 will be applied.

After updating the program, add license keys (see page [95](#)) again.

Installing program update packages

When Kaspersky Lab issues software updates, you can install the program update packages.

Prior to installing program update packages, you are advised to first create a backup copy of the current state of the program (see page [369](#)) and download it to the hard drive of your computer from the program administrator menu. If an error occurs during installation of a program update package or if it becomes necessary to reinstall Kaspersky Anti Targeted Attack Platform, you will be able to use the saved copy of the program.

► *To download an archive with the program update package to the server hosting the Central Node component, proceed as follows:*

1. Log in to the management console of the server with the Central Node component via the SSH protocol or through a terminal.
2. When the system prompts you, enter the administrator user name and the password that was specified during installation of the program.

The program administrator menu is displayed.

3. In the program administrator menu, select Technical Support Mode.
4. Press **ENTER**.

The Technical Support Mode confirmation window opens.

5. Select **Yes** and press **ENTER**.
6. Run the command

```
scp <program update package name>.ktgz <Central Node server admin user name>@<IP address of server with Central Node component>
```

For example, you can run the command `apt-system-3.6.0-tr-patch-122.ktgz`
`admin@10.10.10.1`

You can proceed to install the upgrade package.

► *To install the upgrade package:*

1. Log in to the management console of the server with the Central Node component via the SSH protocol or through a terminal.
2. When the system prompts you, enter the administrator user name and the password that was specified during installation of the program.

The program administrator menu is displayed.

3. In the program administrator menu, select **System Administration**.
4. Press **ENTER**.

The action selection window is displayed.

5. Select **Install patch** and press **ENTER**.

You will see a window containing a list of program upgrade packages available for installation.

6. Select the program update package that you want to install and press **ENTER**.
The action selection window is displayed.
 7. Select **Validate and Install <program update package name>.ktgz** and press **ENTER**.
The upgrade package will be installed. You will be required to restart the server.
 8. Select **Go Back** and press **ENTER**.
The program administrator menu is displayed.
 9. In the program administrator menu, select **Reboot the Machine** and press **ENTER**.
The server with the Central Node component will be restarted.
- Installation of the program update package will be completed.

Interaction with external systems via API

You can set up the integration of Kaspersky Anti Targeted Attack Platform with external systems to scan files that are stored in those systems (see page [380](#)), and to provide access to information about all alerts (see page [384](#)) to the external systems.

External systems interact with Kaspersky Anti Targeted Attack Platform via an API. API method calls are available only to authorized external systems (see page [379](#)).

Interaction between an external system and Kaspersky Anti Targeted Attack Platform

The following scenario is recommended for interaction of an external system with the program:

a. Authorization of the external system

The administrator must create a request to integrate the external system (see page [379](#)) with the program. Then the program administrator must process the request in the web interface of Kaspersky Anti Targeted Attack Platform (see page [214](#)).

b. Call the `POST` method to start a scan (see page [380](#))

c. Call the `GET` method to receive the scan results (see page [381](#))

The API interface is asynchronous, which means that Kaspersky Anti Targeted Attack Platform scans objects in the background instead of immediately upon request of the external system. For this reason, you must periodically send a request from the external system using the `GET` method to receive the scan results. The recommended frequency for sending a request is once per minute.

You can also configure forwarding of notifications (see page [352](#)) about detected objects in the web interface of Kaspersky Anti Targeted Attack Platform.

d. Call the `DELETE` method to delete the scan results (see page [382](#))

You can delete the results of scanning a specified object or all objects.

e. Requesting information about all Kaspersky Anti Targeted Attack Platform alerts

You can get information about all Kaspersky Anti Targeted Attack Platform alerts, not just the objects that are stored in the external system. In the request, you can use filters to get information about objects that satisfy specified criteria.

Creating a request to integrate an external system with Kaspersky Anti Targeted Attack Platform

To begin working with the API, the external system must complete authorization on the Kaspersky Anti Targeted Attack Platform server. For this purpose, you must create an integration request.

► *To create a request to integrate an external system with Kaspersky Anti Targeted Attack Platform:*

1. Generate a unique ID for the external system to interact with the API.

2. Generate a certificate for the external system server.

If you replace a certificate, you must complete authorization again.

3. Call any method while indicating the ID (`sensorId`).

The external system integration request will be displayed in the Kaspersky Anti Targeted Attack Platform web interface (see page [214](#)). Contact the program administrator to process the request.

API for scanning objects of external systems

Kaspersky Anti Targeted Attack Platform provides the HTTPS REST interface for scanning objects saved in external systems.

Working with a cluster

If the external system consists of several servers that are combined into a cluster, it is recommended to use one ID (`sensorId`) for all servers. If this is the case, a single integration request (see page [214](#)) will be displayed for the entire system in the web interface of Kaspersky Anti Targeted Attack Platform. If it is necessary to differentiate the receipt of scan results over individual servers, you can assign a unique instance ID (`sensorInstanceId`) to each server.

Restrictions

The maximum allowed number of object scan requests from external systems and the maximum allowed size of a scanned object are set in the Kaspersky Anti Targeted Attack Platform configuration file.

If the maximum allowed number of simultaneous object scan requests is exceeded, Kaspersky Anti Targeted Attack Platform does not process further requests until the number of object scan requests is less than the maximum allowed number. Until this condition is met, the return code 429 is issued. You must try the scan request again later.

If the maximum allowed object size is exceeded, Kaspersky Anti Targeted Attack Platform does not scan the object. When the `POST` method is called, the return code 413 is issued. You can find out the maximum allowed size of an object by viewing the list of filters using the `GET` method (see page [383](#)).

Scanning objects

The `POST` method is used to scan objects.

Syntax

```
POST "<URL of the server with the Central Node
component>/sensors/<sensorId>/scans"
```

Example

```
curl -X POST "https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-58006b8f6056/scans?sensorInstanceId" -H "accept: application/json"
-H "Content-Type: multipart/form-data" -F "objectType=file" -F
"content=@sample.yaml;type=application/x-yaml" -F "scanId=52e27edc-9aa8-4f37-8b5a-789d334e062a"
```

Parameters

Parameter	Type	Description
<code>sensorId</code>	string	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
<code>sensorInstanceId</code>	string	Unique ID of the external system instance. Servers combined into a cluster are also considered to be instances of an external system. This parameter is optional.
<code>objectType</code>	string	Type of scanned object. Possible value of the parameter: <code>file</code> .
<code>content</code>	file	Contents of the scanned object.
<code>scanId</code>	string	Unique ID of the scan. If this parameter is not defined, viewing scan results is not available.

Returned value

Return code	Description
200	Scan completed successfully.
401	Authorization required.
429	Number of requests exceeded. Repeat the request later.
500	Internal server error. Repeat the request later.

Viewing scan results

The `GET` method is used to view scan results.

Syntax

```
GET "<URL of the server with the Central Node component>/sensors/<sensorId>/scans/state"
```

Example

```
curl -X GET "https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-58006b8f6056/scans/state?sensorInstanceId=instance1&state=detected,notdetected,error,timeout" -H "accept: application/json"
```

Parameters

Parameter	Type	Description
<code>sensorId</code>	string	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
<code>sensorInstanceId</code>	string	Unique ID of the external system instance. If this parameter is not defined, the scan results for all instances will be displayed.
<code>state</code>	array (string element type)	Object scan status. When this parameter is defined, the scan results will be filtered by status. If you specify multiple statuses, separate them with commas. The following parameter values are available: <ul style="list-style-type: none"> • <code>detected</code>; • <code>notdetected</code>; • <code>processing</code>; • <code>error</code>.

Returned value

Return code	Description
200	Scan completed successfully.
204	No contents.
404	No scan results found for the specified ID.
500	Internal server error. Repeat the request later.

Deleting scan results

The `DELETE` method is used to delete scan results.

Syntax

```
DELETE "<URL of the server with the Central Node component>/sensors/<sensorId>/scans/<scanId>"
```

Example

```
curl -X DELETE "https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-58006b8f6056/scans/52e27edc-9aa8-4f37-8b5a-789d334e062a" -H "accept: application/json"
```

Parameters

Parameter	Type	Description
sensorId	string	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
scanId	string	Unique ID of the scan. If this parameter is not defined, the scan results for all objects will be deleted.

Returned value

Return code	Description
200	Scan completed successfully.
401	Authorization required.
404	No scan results found for the specified ID.
500	Internal server error. Repeat the request later.

Viewing filters

The GET method is used to view filters.

Syntax

```
GET "<URL of the server with the Central Node
component>/sensors/<sensorId>/scans/filters"
```

Example

```
curl -X GET "https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-a00b-438c-b95a-58006b8f6056/scans/filters" -H "accept: application/json"
```

Parameters

Parameter	Type	Description
sensorId	string	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.

Returned value

Return code	Description
200	Scan completed successfully.
401	Authorization required.
500	Internal server error. Repeat the request later.

API for sending alert information to external systems

Kaspersky Anti Targeted Attack Platform provides an API that lets external systems access information about all alerts of the program and not just to scan results for objects stored in these external systems.

In order to receive information only for alerts that satisfy certain conditions, you can specify filters in the request parameters.

The program does not automatically send information about new alerts based on prior requests. A new request must be sent to receive up-to-date information.

Special considerations for operation in the distributed solution

If the program operates in the distributed solution mode, an external system can complete the authorization procedure only on the SCN server. Authorization on the PCN server is not available.

In this case, an external system cannot receive information about all alerts registered in the infrastructure using a single request. This limitation arises because the common database which contains records about all alerts in the infrastructure is stored on the PCN server. To receive information about all alerts, the external system must query each SCN server separately.

Requesting alert information

To get information about program alerts, use the `GET` method.

Syntax

```
curl -X GET "<URL of the server with the Central Node  
component>/sensors/<sensorId>/detects?<parameters>"
```

Example

Example:

```
curl -X GET "https://api.example.com/kata/scanner/v1/sensors/dd62a4ee-  
a00b-438c-b95a-  
58006b8f6056/detects?detect_type=am,sb&limit=100&token=7b226f666673657422  
3a20307d" -H "accept: application/json"
```


Parameters

Parameter	Type	Description
<code>sensorId</code>	String	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
<code>detect_type</code>	Array	Technology that was used to generate the alert. You can specify a comma-separated list of technologies. Possible values: <ul style="list-style-type: none"> • <code>am</code> – Anti-Malware Engine • <code>sb</code> – Sandbox • <code>yara</code> – YARA • <code>url_reputation</code> – URL Reputation • <code>ids</code> – Intrusion Detection System • <code>taa</code> – Targeted Attack Analyzer If the parameter is not specified, information about all alerts is provided.
<code>limit</code>	Integer	Number of objects for which information is provided in response to the request. Allowed values: integers from 1 to 10000. The default value is <code>1000</code> .
<code>token</code>	String	Request ID. If this parameter is specified, a repeated request does not show alert information that was obtained by prior requests. This helps avoid the duplication of information about the same alerts in case of repeated requests. If this parameter is not specified, information about all alerts is provided.

Returned value

Return code	Description
200	Operation completed successfully.
400	Incorrect parameters.
429	Number of requests exceeded.
401	Authorization required.
500	Internal server error. Repeat the request later.

Scope of transmitted data

Information that is transmitted for each alert is listed in the following table.

Table 22. Scope of transmitted alert data

Parameter	Value	Description
alertID	Integer value.	Alert ID.
eventTimeStamp	Date and time.	Event time.
detectTimestamp	Date and time.	Time when alert information was recorded in the Kaspersky Anti Targeted Attack Platform database.
importance	One of the following values: <ul style="list-style-type: none"> • high • medium • low 	Alert importance.
objectSource	One of the following values: <ul style="list-style-type: none"> • web • mail • endpoint • external • dns 	Source of the detected object.
technology	One of the following values: <ul style="list-style-type: none"> • am – Anti-Malware Engine • sb – Sandbox • yara – YARA • url_reputation – URL Reputation • ids – Intrusion Detection System • taa – Targeted Attack Analyzer 	Technology that was used to detect the object.
objectType	One of the following values: <ul style="list-style-type: none"> • file. • URL. • host (for remote domains or hosts). 	Type of detected object
object	Depends on the type of detected object.	Data on the detected object (see page 386).
detection	Depends on the technology that was used to detect the object.	Data on detected threats (see page 389)
details	Depends on the source of detected object.	Data on the environment of detected objects (see page 391).

Data on detected objects

The scope of transmitted data on detected objects depending on the type of the object is listed in the following table.

Table 23. Data on detected objects

	Parameter	Data type	Description	Example
file	processedObject.MD5	MD5	MD5 hash of the file or composite object that was sent for scanning.	1839a1e9621c58dadf782e131df3821f
	processedObject.SHA256	SHA 256	SHA256 hash of the file or composite object that was sent for scanning.	7bbfc1d690079b0c591e146c4294305da1ce857e12db40f4318598fdb503a47
	processedObject.fileName	String	Name of the file or composite object that was sent for scanning.	EICAR-CURE.com
	processedObject.fileType	String	Type of the file or composite object that was sent for scanning.	GeneralTxt
	processedObject.fileSize	Integer	Size of the file or composite object that was sent for scanning, in bytes.	184
	detectedObject.MD5	MD5	MD5 hash of the file (simple object or file within a composite object) in which the threat was detected.	1839a1e9621c58dadf782e131df3821f

	Parameter	Data type	Description	Example
	<code>detectedObject.fileName</code>	String	Name of the file (simple object or file within a composite object) in which the threat was detected.	EICAR-CURE.com
	<code>detectedObject.fileSize</code>	Integer	Size of the file (simple object or file within a composite object) in which the threat was detected, in bytes.	184

	Parameter	Data type	Description	Example
U R L	detectedObject	String	URL of the detected object.	<code>http://example.com/link</code>
h o s t	detectedObject	Array	List of domains to which detected objects belong. <ul style="list-style-type: none"> • For the TAA technology, only one domain is listed. • For the URL technology, as well as for objects with the objectSource=dnsp parameter, the list can contain several domains. 	<code>example.org, example.net</code>

Data on detected threats

The scope of transmitted data on detected threats depending on the technology that was used to generate the alert is listed in the table below.

Table 24. Data on detected threats

Technology	Parameter	Description	Data type	Example
One of the following technologies: <ul style="list-style-type: none"> • Anti-Malware Engine. • YARA. • Intrusion Detection System. 	detect	List of detected threats.	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	dataBaseVersion	Version of databases used to scan the file.	Integer	201811190706
Sandbox	detect	List of detected threats.	Array	HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic
	image	Name of the virtual machine image where the file was scanned.	String	Win7
	dataBaseVersion	Database version in the following format: <version of the program databases which were used to scan the file> / <version of the IDS module databases>.	Integer	201902031107/ 201811190706
URL Reputation	detect	List of URL Reputation categories for the detected object (for objects of type URL or host).	Array	Phishing host, Malicious host, Botnet C&C (Backdoor.Win32.Mokes)
Targeted Attack Analyzer	detect	Name of the TAA module alert.	The only possible value is Suspicious remote host activity	Suspicious remote host activity

Data on the environment of detected objects

The scope of transmitted data on the environment of detected objects depending on the source of the object is listed in the following table.

Table 25. Data on the environment of detected objects

Source of the object	Parameter	Description	Data type	Example
web	sourceIP	IP address of the computer that established the connection.	IP address	192.0.2.0
	sourceHostName	Name of the computer that established the connection.	String	example.com
	destinationIp	IP address of the computer with which the connection was established.	IP address	198.51.100.0
	destinationPort	Port of the computer with which the connection was established.	Integer	3128

Source of the object	Parameter	Description	Data type	Example
	URL	URL of the web resource that was accessed. IDS technology alerts do not have this parameter. For URL technology alerts, this parameter has the same value as the <code>detectedObject</code> parameter.	String	<code>https://example.com:443/</code>
	<code>method</code>	HTTP request method.	String	<code>Connect</code>
	<code>referrer</code>	URL from which the redirect was made.	String	<code>https://example.com:443/</code>
	<code>agentString</code>	User agent header of the HTTP request that contains the name and version of the client application.	String	<code>Mozilla/4.0</code>
mail	<code>mailFrom</code>	Sender's email address.	String	<code>sender@example.com</code>
	<code>mailTo</code>	Comma-separated list of recipient email addresses.	Array	<code>recipient1@example.com, recipient2@example.com</code>

Source of the object	Parameter	Description	Data type	Example
	subject	Subject of the message.	String	'You are the winner'
	messageId	Email message ID.	String	1745028736.156014.1542897410859.JavaMail.svc_jira_pool@hqconflapp2
<ul style="list-style-type: none"> • end point • external 	hostName	Name of the computer on which the alert was generated.	String	computername.example.com
	IP	IP address of the computer on which the alert was generated.	IP address	198.51.100.0
dns	sourceIp	IP address of the computer which initiated the DNS connection.	IP address	192.0.2.0
	destinationIp	IP address of the computer with which the DNS connection was established (typically, a DNS server).	IP address	198.51.100.0
	destinationPort	Port of the computer with which the DNS connection was established (typically, a DNS server).	Integer	3128
	dnsMessageType	Type of the DNS message: <ul style="list-style-type: none"> • Request • Response 	String	Request

Source of the object	Parameter	Description	Data type	Example
	dnsRequest Type	One of the following DNS request types: <ul style="list-style-type: none">• A.• AAA.• CNAME.• MX.	String	MX
	domainToBe Resolved	Domain name from the DNS request.	String	example.com

Contacting the Technical Support Service

This section describes the ways to get technical support and the terms on which it is available.

How to obtain Technical Support

If you cannot find a solution to your problem in the program documentation or in one of the sources of information about the program, we recommend that you contact Technical Support. Technical Support specialists will answer your questions about installing and using the program.

Before contacting Technical Support, please read the technical support rules (<http://support.kaspersky.com/support/rules>).

You can contact Technical Support in one of the following ways:

- By calling Technical Support (<http://support.kaspersky.com/b2b>).
- By sending a request to Technical Support through the Kaspersky CompanyAccount portal (<https://companyaccount.kaspersky.com>).

Technical support by phone

In most regions around the world, you can call Technical Support representatives. You can find information on how to receive technical support in your region and contact information for Technical Support on the Kaspersky Lab Technical Support website (<http://support.kaspersky.com/b2b>).

Before contacting Technical Support, please read the technical support rules (<http://support.kaspersky.com/support/rules>).

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab specialists via online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky Lab specialists and store a history of electronic requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

The portal Kaspersky CompanyAccount is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Technical Support website (https://support.kaspersky.com/faq/companyaccount_help).

Sources of information about the program

This section lists the sources of information about the program.

You can select the most suitable information source, depending on the issue's level of importance and urgency.

Glossary

A

Advanced persistent threat (APT)

A sophisticated targeted attack against the corporate IT infrastructure that simultaneously uses different methods to infiltrate the network, hide on the network, and gain unobstructed access to confidential data.

Alternate data stream

Data streams of the NTFS file system (alternate data streams) are intended for additional attributes or information on a file.

Each file in the NTFS file system consists of a set of streams. The main stream contains the file contents. The other (alternate) streams are intended for metadata. Streams can be created, deleted, individually saved, renamed, and can even be run as a process.

Alternate streams can be used by hackers for concealed transmission or receipt of data from a computer.

Anti-Malware Engine

Program engine. Scans files and objects for viruses and other threats to the corporate IT infrastructure using anti-virus databases.

B

Backdoor program

A program planted by hackers on a compromised computer in order to be able to access this computer in the future.

C

Central Node

Program component. Scans data, analyzes the behavior of objects, and publishes analysis results in the web interface of the program.

Communication channel bandwidth

The highest possible speed of information transfer in the specific communication channel.

CSRF attack

Cross-Site Request Forgery (also referred to as an "XSRF attack"). Attack on website users by exploiting vulnerabilities of the HTTP protocol. The attack enables actions to be performed under the guise of an authorized user of a vulnerable website. For example, under the guise of an authorized user of a vulnerable website, a hacker can covertly send a request to the server of an external payment system to transfer money to the hacker's account.

D

Distributed solution

Two-level hierarchy of servers with Central Node components installed. This hierarchy allocates a master control server (*Primary Central Node (PCN)*) and slave servers (*Secondary Central Nodes (SCN)*).

Dump

Contents of the working memory of a process or the entire RAM of the system at a specified moment of time.

E

End User License Agreement

Binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the program.

Endpoint Sensors

Program component. Installed on separate computers that belong to the corporate IT infrastructure and run the Microsoft Windows operating system. Continuously monitors processes running on those computers, active network connections, and files that are modified.

I

ICAP data

Data received by the ICAP protocol (Internet Content Adaptation Protocol). This protocol allows filtering and modifying data of HTTP requests and HTTP responses. For example, it allows scanning data for viruses, blocking spam, and denying access to personal resources. The ICAP client is normally a proxy server that interacts with the ICAP server by the ICAP protocol. Kaspersky Anti Targeted Attack Platform receives data from the proxy server of your organization after this data was processed on the ICAP server.

Intrusion Detection System

Program module. Scans the Internet traffic for signs of intrusions into the corporate IT infrastructure.

IOA

Indicator of Attack. Description of suspicious behavior of objects within a corporate IT infrastructure that may indicate a targeted attack on that organization.

IOA rule

One sign of suspicious behavior of an object in the corporate IT infrastructure that causes Kaspersky Anti Targeted Attack Platform to consider an event to be an alert. An IOA rule contains a description of a sign of an attack and recommended countermeasures.

IOC

Indicator of Compromise. A set of data about a malicious object or malicious activity.

IOC file

File containing a set of IOC indicators; Kaspersky Anti Targeted Attack Platform considers the event to be an alert if it matches these indicators. The likelihood of an alert may increase if a scan detects exact matches between the data of an object and several IOC files.

K

Kaspersky Anti Targeted Attack Platform

Solution designed for the protection of a corporate IT infrastructure and timely detection of threats such as *zero-day attacks*, *targeted attacks*, and complex targeted attacks known as *advanced persistent threats* (hereinafter also referred to as "APT").

Kaspersky Private Security Network

A solution that allows users of Kaspersky Lab anti-virus applications to access Kaspersky Security Network databases without sending data from their computers to Kaspersky Security Network servers.

Kaspersky Secure Mail Gateway

A solution designed for protection of incoming and outgoing email against malicious objects and spam, and for content filtering of messages. The solution lets you deploy a virtual mail gateway and integrate it into the existing corporate mail infrastructure. An operating system, mail server, and Kaspersky Lab anti-virus application are preinstalled on the virtual mail gateway.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

KATA

Kaspersky Anti Targeted Attack. Functional block of the Kaspersky Anti Targeted Attack Platform program, which provides perimeter security for the enterprise IT infrastructure.

KEDR

Kaspersky Endpoint Detection and Response. Functional block of the Kaspersky Anti Targeted Attack Platform program, which provides protection for the local area network of the organization.

L

Local reputation database of KPSN

Database of the reputations of objects (files or URLs) that is stored on the Kaspersky Private Security Network server but not on Kaspersky Security Network servers. Local reputation databases are managed by the KPSN administrator.

M

Malicious web addresses

URLs of resources distributing malicious software.

Mirrored traffic

A copy of traffic redirected from one switch port to another port of the same switch (local mirroring) or to a remote switch (remote mirroring). The network administrator can configure which part of traffic should be mirrored for transmission to Kaspersky Anti Targeted Attack Platform.

MITM attack

Man in The Middle. An attack on the IT infrastructure of an organization in which a hacker hijacks the communication link between two access points, relays it, and modifies the connection between these access points if necessary.

MITRE technique

The MITRE ATT&CK <https://attack.mitre.org/> (Adversarial Tactics, Techniques & Common Knowledge) database contains descriptions of hacker behavior based on the analysis of real attacks. It is a structured list of known hacker techniques represented as a table.

Multitenancy

Operation mode in which the program can be used to protect the infrastructure of several organizations simultaneously.

N

New generation threats

Corporate IT infrastructure threats capable of overwriting, altering, encrypting, or distorting their code to a point where matches against signatures can no longer be detected by a security system.

NTP server

Precision time server using the Network Time Protocol.

O

Open IOC

An open, XML-based standard for describing indicators of compromise containing over 500 different indicators of compromise.

P

Phishing URL addresses

URL addresses of resources designed to obtain unauthorized access to confidential data of users. Phishing is usually aimed at stealing various financial data.

S

Sandbox

Program component. Starts virtual images of operating systems. Starts files in these operating systems and tracks the behavior of files in each operating system to detect malicious activity and signs of targeted attacks to the corporate IT infrastructure.

Sensor

Program component. Receives data.

SIEM system

Security Information and Event Management System. Solution for managing information and events in an organization's security system.

Signature

Code in information protection databases that contains a description of known threats.

SPAN

Switch Port Analyzer. Technology for mirroring traffic from one port to another.

Syslog

The standard for sending and recording messages about events occurring in the system employed on UNIX™ and GNU/Linux platforms.

T

Targeted attack

Attack that targets a specific person or organization. Unlike mass attacks by computer viruses designed to infect as many computers as possible, targeted attacks can be aimed at infecting the network of a specific organization or even a separate server within the corporate IT infrastructure. A dedicated Trojan program can be written to stage each targeted attack.

Targeted Attack Analyzer

Program module. Performs statistical analysis and monitors network activity of software installed on computers of the corporate LAN. Searches for signs of network activity that the user of Kaspersky Anti Targeted Attack Platform is advised to direct his/her attention, as well as signs of targeted attacks to the corporate IT infrastructure.

TLS encryption

Encryption of connection between two servers, which ensures secure transmission of data between servers on the Internet.

Tracing

The program is run in debugging mode; after each command is executed, the program is stopped and the result of this step is displayed.

V

VIP status

Status of alerts with special access permissions. For example, alerts with the VIP status cannot be viewed by users with the Security officer role.

Y

YARA

Program module. Scans files and objects for signs of targeted attacks on the corporate IT infrastructure using YARA Rules databases created by users of Kaspersky Anti Targeted Attack Platform.

YARA Rules

A publicly available classification of malware, which contains signatures of signs of targeted attacks and intrusions into the corporate IT infrastructure, which is used by Kaspersky Anti Targeted Attack Platform to scan files and objects.

Z

Zero-day attack

An attack targeting the corporate IT infrastructure by exploiting zero-day vulnerabilities in software. These are software vulnerabilities that hackers find and exploit before the software vendor has a chance to release a patch.

Zero-day vulnerability

A software vulnerability that hackers find and exploit before the software vendor has a chance to release a patch with fixed program code.

AO Kaspersky Lab

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

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

Kaspersky Lab 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 3000 qualified specialists.

Products. Kaspersky Lab's 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 Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's 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 signatures for these threats in databases used by Kaspersky Lab applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. 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, ZyXEL. Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab 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 Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab'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 Lab website: <https://www.kaspersky.com>

Virus encyclopedia: <https://securelist.com/>

Kaspersky VirusDesk: <https://virusdesk.kaspersky.com/> (for scanning suspicious files and websites)

Kaspersky Lab user community: <https://community.kaspersky.com>

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt, in the program installation folder.

Trademark notices

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

AMD is a trademark of Advanced Micro Devices, Inc.

Apple and Safari are trademarks of Apple Inc.

Citrix and XenServer are trademarks of Citrix Systems, Inc. and/or affiliated companies registered with the Patent Office of United States and other countries.

ESET and ESET NOD32 are trademarks or registered trademarks of ESET, spol. s r.o.

Android and Google Chrome are trademarks of Google, Inc.

FusionCompute, FusionSphere, and HUAWEI are registered trademarks of Huawei Technologies Co., Ltd in China and other countries.

Intel and Core are trademarks of Intel Corporation registered in the United States of America and elsewhere.

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

Mozilla and Firefox are trademarks of the Mozilla Foundation.

Active Directory, Excel, Hyper-V, Power Point, Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries.

CentOS is a trademark of Red Hat, Inc.

Red Hat Enterprise Linux is a trademark of Red Hat Inc. registered in the United States of America and other countries.

Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

Trend Micro is a trademark of Trend Micro.

VMware ESXi and VMware vSphere are trademarks of VMware, Inc or trademarks of VMware, Inc. registered in the United States or other jurisdictions.

UNIX is a trademark registered in the United States and elsewhere and is used under license from X/Open Company Limited.