kaspersky

# Kaspersky Anti Targeted Attack Platform

© 2026 AO Kaspersky Lab

# Contents


Kaspersky Anti Targeted Attack Platform Help

Kaspersky Anti Targeted Attack Platform

- What's new
- About Kaspersky Threat Intelligence Portal
- Distribution kit
- Hardware and software requirements
  - Requirements for Kaspersky Endpoint Agent
  - Compatibility of Kaspersky Endpoint Agent (Endpoint Sensors) versions with Kaspersky Anti Targeted Attack Platform versions
  - Compatibility of the Kaspersky Endpoint Agent (Endpoint Sensors) component versions with Kaspersky Endpoint Security versions
  - Compatibility of Kaspersky Endpoint Agent with other programs
- Limitations of the current version of the program

About data provision

- Data of the Central Node and Sensor components
  - Traffic data of the Sensor component
  - Data in alerts
  - Data in events
  - Data in reports
  - Data on objects in Storage and Quarantine
  - Data on program settings
- Sandbox component data
- Data transmitted between program components
- Data of Kaspersky Endpoint Agent
  - Data received from the Central Node component
  - Data in fields of Windows Event Log events of Kaspersky Endpoint Agent
  - Data in Kaspersky Endpoint Agent requests to Kaspersky Anti Targeted Attack Platform
  - Service data of Kaspersky Endpoint Agent
  - Data contained in Kaspersky Endpoint Agent trace files and dumps
  - Data sent to Kaspersky if KSN and KMP Statements are accepted
  - Data in alerts and events
  - Data contained in task completion reports
  - Data contained in an install log
  - Data on files that are blocked from starting
  - Data related to the performance of tasks

Program licensing

- About the End User License Agreement
- About the license
- About the license certificate
- About the key
- About the key file
- Viewing information about the license and added keys
- Viewing the text of the End User License Agreement in the web interface of the Central Node
- Viewing the text of the Privacy Policy in the web interface of the Central Node

Viewing information about the third-party code used in the program
Viewing the text of the End User License Agreement in the web interface of the Sandbox
Viewing the text of the End User License Agreement on a computer with Kaspersky Endpoint Agent
Adding a key
Replacing a key
Removing a key
Program modes based on the license
Program architecture
Sensor component
Central Node component
Sandbox component
Kaspersky Endpoint Agent component
Operation of the program
Distributed solution and multitenancy mode
Distributed mode and multitenancy transition scenario
Modifications of program settings for distributed solution mode and multitenancy
Assigning the PCN role to a server
Assigning the SCN role to a server
Processing SCN to PCN connection requests
Viewing information about organizations, PCN and SCN servers
Adding an organization to the PCN server
Removing an organization from the PCN server
Renaming an organization on the PCN server
Disconnecting an SCN from PCN
Modifications of program settings for disconnecting an SCN from PCN
Decommissioning an SCN server
Sizing Guide
Common scenarios for deployment and installation of program components
Two-server deployment scenario
Three-server deployment scenario.
Scenario of deployment on four or more servers.
Scenario for deploying KEDR functionality with a Sandbox component
Scenario for deploying KEDR functionality without a Sandbox component
Sizing calculator
Calculations for the Sensor component
Calculations for the Central Node component
Calculations for the Sandbox component
Installing and performing initial configuration of the solution
Preparing for installing program components
Preparing the IT infrastructure for program components installation
Preparing the IT infrastructure for integration with a mail server used for receiving messages via POP3
Preparing the IT infrastructure for integration with a mail server used for receiving messages via SMTP
Preparing the virtual machine for installing the Sandbox component
Procedure for installing and configuring program components
Installation: Sandbox component
Step 1. Viewing the End User License Agreement and Privacy Policy
Step 2. Selecting a disk for installing the Sandbox component

- Step 3. Assigning the host name
- Step 4. Selecting the management network interface in the list
- Step 5. Assigning the address and network mask of the controlling interface
- Step 6. Adding DNS server addresses
- Step 7. Configuring a static network route
- Step 8. Configuring the minimum password length for the Sandbox administrator password
- Step 9. Creating the Sandbox administrator account

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

- Step 1. Viewing the End User License Agreement and Privacy Policy
- Step 2. Selecting a disk for installing the Central Node and Sensor components
- Step 3. Selecting a server role
- Step 4. Configuring the minimum password length for the administrator password
- Step 5. Creating an account for working in the administrator menu and in the server management console
- Step 6. Assigning the host name
- Step 7. Enabling a network interface for the first time
- Step 8. Assigning the address and subnet mask of the management interface
- Step 9. Configuring the default network route
- Step 10. Configuring DNS settings
- Step 11. Configuring proxy server connection settings
  - Enabling and disabling the use of a proxy server
  - Configuring proxy server connection settings
  - Enabling and disabling the use of a proxy server when connecting to local addresses
- Step 12. Setting the time zone
- Step 13. Configuring time synchronization with an NTP server
- Step 14. Configuring integration with the Sandbox component
- Step 15. Allocating the disk for the Targeted Attack Analyzer component's database
- Step 16. Creating an administrator account for the web interface of Kaspersky Anti Targeted Attack Platform
- Step 17. Configuring receipt of mirrored traffic from SPAN ports
  - Selecting network interfaces for receiving mirrored traffic from SPAN ports
  - Selecting network protocols for receiving mirrored traffic from SPAN ports
  - Configuring the transmission of HTTP traffic details for IDS alerts
- Step 18. Configuring integration with a proxy server via ICAP
- Step 19. Configuring integration with a mail server via POP3
- Step 20. Configuring integration with a mail server via SMTP

Installing and configuring the Sensor component on a separate server

- Step 1. Viewing the End User License Agreement and Privacy Policy
- Step 2. Selecting a disk for installing the Sensor component
- Step 3. Selecting a server role
- Step 4. Configuring the minimum password length for the administrator password
- Step 5. Creating an account for working in the administrator menu and in the server management console
- Step 6. Assigning the host name
- Step 7. Enabling a network interface for the first time
- Step 8. Assigning the address and subnet mask of the management interface
- Step 9. Configuring the default network route
- Step 10. Configuring DNS settings

Step 11. Configuring proxy server connection settings
Enabling and disabling the use of a proxy server
Configuring proxy server connection settings
Enabling and disabling the use of a proxy server when connecting to local addresses
Step 12. Setting the time zone
Step 13. Configuring time synchronization with an NTP server
Step 14. Connecting to the server with the Central Node component
Step 15. Selecting the Central Node server as the source of Sensor component database updates
Step 16. Configuring receipt of mirrored traffic from SPAN ports
Selecting network interfaces for receiving mirrored traffic from SPAN ports
Selecting network protocols for receiving mirrored traffic from SPAN ports
Configuring the transmission of HTTP traffic details for IDS alerts
Step 17. Configuring integration with a proxy server via ICAP
Step 18. Configuring integration with a mail server via POP3
Step 19. Configuring integration with a mail server via SMTP
Configuring the integration of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent
Configuring the trusted connection of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent
Configuring the connection with the Central Node server without validating the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.
Configuring the connection with the Sensor server without validating the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.
Configuring the connection with the Central Node server with validation of the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.
Configuring the connection with the Sensor server with validation of the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.
Downloading the TLS certificate of the Central Node server
Generating a TLS certificate for the Central Node server in the web interface of Kaspersky Anti Targeted Attack Platform
Uploading an independently prepared TLS certificate for the Central Node server using the web interface of Kaspersky Anti Targeted Attack Platform.
Uploading a TLS certificate of the Central Node server or Sensor to Kaspersky Endpoint Agent
Enabling the validation of the Kaspersky Endpoint Agent TLS certificate in the web interface of Kaspersky Anti Targeted Attack Platform
Generating a TLS certificate of Kaspersky Endpoint Agent in the web interface of Kaspersky Anti Targeted Attack Platform and downloading a cryptographic container
Uploading an independently prepared TLS certificate of Kaspersky Endpoint Agent using the web interface of Kaspersky Anti Targeted Attack Platform.
Viewing the table of Kaspersky Endpoint Agent TLS certificates in the web interface of Kaspersky Anti Targeted Attack Platform
Filtering and searching Kaspersky Endpoint Agent TLS certificates in the web interface of Kaspersky Anti Targeted Attack Platform
Deleting Kaspersky Endpoint Agent TLS certificates in the web interface of Kaspersky Anti Targeted Attack Platform
Configuring the validation of the Kaspersky Endpoint Agent TLS certificate by the Central Node server and uploading a cryptographic container to Kaspersky Endpoint Agent
Configuring traffic redirection from Kaspersky Endpoint Agent to the Sensor server
Enabling and disabling traffic redirection from Kaspersky Endpoint Agent to the Sensor server
Authorizing the Sensor component on a Central Node server
Generating a TLS certificate for the Sensor server in the administrator menu of the Sensor server
Uploading an independently prepared TLS certificate for the Sensor server in the administrator menu of the Sensor server

Downloading the TLS certificate of the Sensor server to your computer
Configuring the integration and trusted connection with Kaspersky Anti Targeted Attack Platform on the Kaspersky Endpoint Agent side
Getting started with the program
Getting started with the program web interface
Getting started with the program administrator menu
Getting started with the program in Technical Support Mode
Managing accounts of program administrators and users
Creating an administrator account for the program web interface
Creating a user account for the program web interface
Changing access rights of a program web interface user account
Enabling and disabling an administrator account or user account of the program web interface
Changing the password of a program administrator or user account
Changing the password of your account
Participation in Kaspersky Security Network and use of Kaspersky Private Security Network
Viewing the KSN Statement and configuring participation in KSN
Enabling the use of KPSN
Configuring a connection to a local reputation database of KPSN
Configuring information to be saved to a local reputation database of KPSN
Declining participation in KSN and use of KPSN
Managing the Sandbox component through the web interface
Updating the Sandbox component databases
Updating databases manually
Selecting a database update source
Enabling and disabling a proxy server for database update
Configuring proxy server connection settings for database update
Configuring connection between the Sandbox and Central Node components
Creating a request for connection to Sandbox in the Central Node administrator menu
Processing connection requests from the Central Node servers in the Sandbox web interface
Configuring the Sandbox component network interfaces
Configuring DNS settings
Configuring settings of the management network interface
Configuring settings of a network interface used for Internet access of processed objects
Adding, changing and removing static network routes
Updating the Sandbox system
Setting the Sandbox system date and time
Installing and configuring images of operating systems and software required for the operation of the Sandbox component
Downloading ISO images of operating systems and software required for the operation of the Sandbox component
Creating virtual machines with images of operating systems and software required for the operation of the Sandbox component
Installing virtual machines with images of operating systems and software required for the operation of the Sandbox component
Deleting all pending virtual machines
Setting the maximum number of simultaneously running virtual machines
Downloading the Sandbox system log to the hard drive
Exporting Sandbox settings
Importing Sandbox settings

Restarting the Sandbox server
Powering off the Sandbox server
Changing the Sandbox administrator account password
For an administrator: Getting started with the program web interface
Kaspersky Anti Targeted Attack Platform Interface
Monitoring program operation
About widgets and layouts
Selecting an organization and a server to manage in the Dashboard section
Adding a widget to the current layout
Moving a widget in the current layout
Removing a widget from the current layout
Saving a layout to PDF
Configuring the period for displaying data in widgets
Monitoring the receipt and processing of incoming data
Monitoring the queues for data processing by program modules and components
Monitoring the processing of data by the Sandbox component
Viewing the working condition of modules and components of the program
Managing Central Node, PCN, or SCN servers using the program web interface
Configuring the date and time on the server
Powering off and restarting the server
Generating or uploading a TLS certificate of the server
Downloading the TLS certificate of the server
Assigning a server DNS name
Configuring DNS settings
Configuring settings of the network interface
Configuring the default network route
Configuring proxy server connection settings
Managing the Sensor component
Processing a connection request from the Sensor component
Viewing the table of servers with the Sensor component
Configuring the maximum size of a scanned file
Configuring receipt of mirrored traffic from SPAN ports
Configuring integration with a mail server via SMTP
Configuring TLS encryption of connections with a mail server via SMTP
Enabling integration with a proxy server via ICAP
Configuring integration with a mail server via POP3
Managing Kaspersky Endpoint Agent host information
Selecting an organization to manage in the Endpoint Agents section
Viewing the Kaspersky Endpoint Agent host table on a standalone Central Node server
Viewing the Kaspersky Endpoint Agent host table in distributed solution and multitenancy mode
Viewing information about a host
Filtering and searching hosts with Kaspersky Endpoint Agent by host name
Filtering and searching hosts with Kaspersky Endpoint Agent that have been isolated from the network
Filtering and searching hosts with Kaspersky Endpoint Agent by PCN and SCN server names
Filtering and searching hosts with Kaspersky Endpoint Agent by computer IP address
Filtering and searching hosts with Kaspersky Endpoint Agent by operating system version on the computer
Filtering and searching hosts with Kaspersky Endpoint Agent by Kaspersky Endpoint Agent version

Filtering and searching hosts with Kaspersky Endpoint Agent based on their activity
Quickly creating a filter for hosts with Kaspersky Endpoint Agent
Resetting the hosts with Kaspersky Endpoint Agent filter
Configuring activity indicators of Kaspersky Endpoint Agent
Supported interpreters and processes
Configuring integration with the Sandbox component
Viewing the table of servers with the Sandbox component
Creating a request to connect to the server with the Sandbox component
Enabling and disabling a connection with the Sandbox component
Deleting a connection with the Sandbox component
Configuring integration with external systems
Viewing the table of external systems
Processing a request from an external system
Removing an external system from the list of those allowed to integrate
Configuring the priority for processing traffic from mail sensors
Configuring integration with Kaspersky Managed Detection and Response
Enabling the MDR integration
Disabling the MDR integration
Replacing the MDR configuration file
Configuring integration with an SIEM system
Enabling and disabling event logging to a local log
Enabling and disabling event logging to a remote log
Configuring the main settings for SIEM system integration
Enabling and disabling TLS encryption of the connection with the SIEM system
Uploading a TLS certificate
Content and properties of syslog messages about alerts
Configuring server settings for delivery of notifications
Database Update
Selecting a database update source
Updating databases manually
Creating a list of passwords for archives
For a security officer: Getting started with the program web interface
Kaspersky Anti Targeted Attack Platform Interface
Selecting an organization to manage in the web interface of the program
Monitoring program operation
About widgets and layouts
Adding a widget to the current layout
Moving a widget in the current layout
Removing a widget from the current layout
Saving a layout to PDF
Configuring the period for displaying data in widgets
Configuring the widget display scale
Main principles of working with "Alerts" widgets
Viewing the working condition of modules and components of the program
Table of alerts

Filtering, sorting, and searching alerts
Filtering alerts by VIP status
Filtering and searching alerts by time
Filtering alerts by level of importance
Filtering and searching alerts by categories of objects detected
Filtering and searching alerts by obtained information
Filtering and searching alerts by source address
Filtering and searching alerts by destination address
Filtering and searching alerts by server name
Filtering and searching alerts by technology name
Filtering and searching alerts by the status of their processing by the user
Sorting alerts in the table
Quickly creating an alert filter
Clearing an alert filter
Viewing alerts
Viewing alert details
General information about an alert of any type
Information in the Object information section
Information in the Alert information section
Information in the Scan results section
Information in the IDS rule section
Information in the Network event section
Scan results in Sandbox
IOC scan results
Information in the Hosts section
Information in the Change log section
Sending alert data
Recommendations for processing alerts
Recommendations for processing AM alerts
Recommendations for processing SB alerts
Recommendations for processing YARA alerts
Recommendations for processing IOC alerts
Recommendations for processing IDS alerts
User actions performed on alerts
Assigning several alerts to a specific user
Assigning alerts to yourself or to another user
Marking the completion of single alert processing
Marking the completion of alerts processing
Modifying the status of VIP alerts
Adding a comment to an alert
Events database threat hunting
Searching events in design mode
Searching events in source code mode
Changing the event search conditions
Searching events by processing results in EPP programs
Uploading an IOC file and searching for events based on conditions defined in the IOC file
Creating a user-defined TAA (IOA) rule based on event search conditions

Event information
Viewing the table of events
Viewing information about an event
Information about events in the tree of events
Viewing parent process information in the tree of events
Viewing information about events initiated by the parent process in the tree of events
Viewing host information in the tree of events
Recommendations for processing events
Following a recommendation to isolate a host
Following a recommendation to prevent a file from running
Following a recommendation to create a task
Information about the "Process started" event
Information about the "Module loaded" event
Information about the "Remote connection" event
Information about the "Prevention rule" event
Information about the "Document blocked" event
Information about the "File created" event
Information about the "Windows log event" event
Information about the "Changes in the registry" event
Information about the "Port listened" event
Information about the "Driver loaded" event
Information about the "Alert" event
Information about the "Alert processing result" event
Information about the "Interpreted file run" event
Information about the "Interactive command input at the console" event
Managing Kaspersky Endpoint Agent host information
Viewing the Kaspersky Endpoint Agent host table on a standalone Central Node server
Viewing the Kaspersky Endpoint Agent host table in distributed solution and multitenancy mode
Viewing information about a host
Filtering and searching hosts with Kaspersky Endpoint Agent by host name
Filtering and searching hosts with Kaspersky Endpoint Agent that have been isolated from the network
Filtering and searching hosts with Kaspersky Endpoint Agent by PCN and SCN server names
Filtering and searching hosts with Kaspersky Endpoint Agent by computer IP address
Filtering and searching hosts with Kaspersky Endpoint Agent by operating system version on the computer
Filtering and searching hosts with Kaspersky Endpoint Agent by Kaspersky Endpoint Agent version
Filtering and searching hosts with Kaspersky Endpoint Agent based on their activity
Quickly creating a filter for hosts with Kaspersky Endpoint Agent
Resetting the hosts with Kaspersky Endpoint Agent filter
Supported interpreters and processes
Network isolation of Kaspersky Endpoint Agent hosts
Creating a network isolation rule
Adding an exclusion from a network isolation rule
Deleting a network isolation rule
Limitations that are relevant to network isolation
Managing tasks
Viewing the task table
Viewing information about a task

- Creating a process termination task
- Creating a program execution task
- Creating a file download task
- Creating a file deletion task
- Creating a file quarantine task
- Creating a quarantined file recovery task
- Creating a copy of a task
- Deleting tasks
- Filtering tasks by creation time
- Filtering tasks by type
- Filtering tasks by name
- Filtering tasks by file name and path
- Filtering tasks by description
- Filtering tasks by server name
- Filtering tasks based on the name of the user that created the task
- Filtering tasks by processing status
- Clearing a task filter

Managing policies (prevention rules)

- Viewing the prevention rule table
- Viewing a prevention rule
- Creating a prevention rule
- Enabling and disabling a prevention rule
- Enabling and disabling presets
- Deleting prevention rules
- Filtering prevention rules by name
- Filtering prevention rules by type
- Filtering prevention rules by file hash
- Filtering prevention rules by server name
- Clearing a prevention rule filter

Managing user-defined rules

- Using indicators of compromise (IOC) and attack (IOA) for Threat Hunting
- Managing user-defined IOC rules
  - Viewing the table of IOC files
  - Viewing information about an IOC file
  - Uploading an IOC file
  - Downloading an IOC file to a computer
  - Enabling and disabling the automatic use of an IOC file when scanning events
  - Deleting an IOC file
  - Searching for alerts in IOC scan results
  - Searching for alerts using an IOC file
  - Filtering and searching IOC files
  - Clearing an IOC file filter
  - Configuring an IOC scan schedule
- Managing user-defined TAA (IOA) rules
  - Viewing the TAA (IOA) rule table
  - Viewing the information of a user-defined TAA (IOA) rule
  - Searching for alerts and events in which TAA (IOA) rules were triggered

Filtering and searching TAA (IOA) rules
Resetting the TAA (IOA) rule filter
Creating a user-defined TAA (IOA) rule based on event search conditions
Importing a user-defined TAA (IOA) rule
Enabling and disabling TAA (IOA) rules
Modifying a user-defined TAA (IOA) rule
Deleting user-defined TAA (IOA) rules
Managing user-defined IDS rules
Importing a user-defined IDS rule
Viewing the information of a user-defined IDS rule
Enabling and disabling the use of an IDS rule when scanning events
Configuring the importance of alerts generated by the user-defined IDS rule
Replacing a user-defined IDS rule
Downloading a user-defined IDS rule file to the computer
Deleting a user-defined IDS rule
Managing YARA rules
Uploading YARA rules
Updating YARA rules
Deleting YARA rules
Managing objects in Storage and Quarantine
Viewing the table of objects that were placed in Storage
Viewing information about an object manually placed in Storage
Viewing information about an object placed in Storage by a task
Downloading objects from Storage
Uploading objects to Storage
Sending objects in Storage for scanning
Deleting objects from Storage
Filtering objects in Storage by object type
Filtering objects in Storage by object description
Filtering objects in Storage based on scan results
Filtering objects in Storage based on the name of Central Node, PCN, or SCN server
Filtering objects in Storage by object source
Filtering objects based on the time they were placed in Storage
Clearing a Storage objects filter
Viewing the table of objects quarantined on computers with Kaspersky Endpoint Agent
Viewing information about a quarantined object
Restoring an object from Quarantine
Obtaining a copy of a quarantined object on a Kaspersky Anti Targeted Attack Platform server
Removing information about the quarantined object from the table
Filtering information about quarantined objects by object description
Filtering information about quarantined objects by host name
Filtering information about quarantined objects by time
Resetting the filter for information about quarantined objects
Managing reports
Creating a template
Creating a report based on a template
Viewing the table of templates and reports

- Viewing a report
- Downloading a report to a local computer
- Editing a template
- Filtering templates by name
- Filtering templates based on the name of the user that created the template
- Filtering templates by creation time
- Clearing a template filter
- Deleting a template
- Filtering reports by creation time
- Filtering reports by name
- Filtering reports by the name of the server with the Central Node component
- Filtering reports based on the name of the user that created the report
- Clearing a report filter
- Deleting a report

Sending notifications

- Viewing the table of rules for sending notifications
- Creating a rule for sending notifications about alerts
- Creating a rule for sending notifications about the operation of program components
- Enabling and disabling a rule for sending notifications
- Modifying a rule for sending notifications
- Deleting a rule for sending notifications
- Filtering and searching notification forwarding rules by rule type
- Filtering and searching notification forwarding rules based on the notification subject
- Filtering and searching notification forwarding rules by email address
- Filtering and searching notification forwarding rules based on their status
- Clearing a notification forwarding rule filter

Managing rules for assigning the VIP status to alerts

- Adding a VIP status assignment rule
- Deleting a VIP status assignment rule
- Modifying a VIP status assignment rule
- Importing a list of VIP status assignment rules
- Exporting a list of VIP status assignment rules
- Filtering and searching by type of VIP status assignment rule
- Filtering and searching by value of VIP status assignment rule
- Filtering and searching by description of VIP status assignment rule
- Clearing a VIP status assignment rule filter

Managing the white list of objects

- Adding a record to the white list
- Removing a record from the white list
- Modifying a record in the white list
- Exporting a white list
- Filtering and searching records in the white list by criterion
- Filtering and searching records in the white list by value
- Clearing a white list record filter

Managing IDS exclusions

- Viewing the list of IDS rules added to exclusions
- Adding an IDS rule to exclusions

Editing the description of an IDS rule added to exclusions
Removing a IDS rule from exclusions
Managing TAA exclusions
Viewing the list of TAA (IOA) rules added to exclusions
Viewing a TAA (IOA) rule added to exclusions
Removing a TAA (IOA) rule from exclusions
Adding a TAA (IOA) rule to exclusions
Creating a list of passwords for archives
Managing Kaspersky Endpoint Agent
Installing and uninstalling Kaspersky Endpoint Agent
Preparing for Kaspersky Endpoint Agent installation
Installing Kaspersky Endpoint Agent
Installing Kaspersky Endpoint Agent using the Installation Wizard
Updating Kaspersky Endpoint Agent from the previous version
Repairing Kaspersky Endpoint Agent
Changes in the system after Kaspersky Endpoint Agent installation
Removing Kaspersky Endpoint Agent using the Installation and Uninstallation Wizard
Installing, restoring and uninstalling the application using the command line
Kaspersky Endpoint Agent activation
Managing Kaspersky Endpoint Agent activation
Functional limitations after the license expiration
Viewing information about the current license
Managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console
Managing Kaspersky Endpoint Agent policies
Creating Kaspersky Endpoint Agent policy
Enabling settings in Kaspersky Endpoint Agent policy
Configuring Kaspersky Endpoint Agent settings
Configuring Kaspersky Endpoint Agent security settings
Configuring user permissions
Enabling Password protection
Enabling and disabling Self-Defense
Configuring Kaspersky Endpoint Agent connection settings to a proxy server
Configuring Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation
Configuring KSN and KMP usage in Kaspersky Endpoint Agent
Configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox
Enabling and disabling integration with Kaspersky Sandbox
Configuring trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent
Configuring the trusted connection on the Kaspersky Sandbox side
Configuring trusted connection on Kaspersky Endpoint Agent side
Updating Kaspersky Sandbox TLS certificate data in Kaspersky Endpoint Agent
Configuring the response timeout of Kaspersky Sandbox and request queue settings
Adding Kaspersky Sandbox servers to Kaspersky Endpoint Agent list
Configuring Threat Response actions of Kaspersky Endpoint Agent to respond to threats detected by Kaspersky Sandbox
Enabling and disabling Threat Response actions
Adding Threat Response actions to the action list of the current policy
Authentication for Threat Response group tasks on the Administration Server

Device protection from legitimate applications that can be used by cybercriminals
Configuring start of Autonomous IOC Scan tasks
Configuring integration between Kaspersky Endpoint Agent and KATA Central Node
Configuring data submission settings
Configuring request throttling settings
Enabling and disabling integration with KATA Central Node
Configuring trusted connection with KATA Central Node
Configuring synchronization settings between Kaspersky Endpoint Agent and KATA Central Node
Configure network isolation settings
About network isolation in Kaspersky Endpoint Agent
About managing network isolation in Kaspersky Endpoint Agent
Enabling and disabling network isolation
Enabling and disabling user notification about network isolation
Configuring automatic disabling of network isolation
Configuring exclusions from network isolation
Configuring quarantine settings in Kaspersky Endpoint Agent
About Kaspersky Endpoint Agent quarantine
About quarantine management in Kaspersky Endpoint Agent
Configuring quarantine settings and restoration of objects from quarantine
Configuring data synchronization with the Administration Server
Managing Kaspersky Endpoint Agent tasks
Creating a local task
Creating a group task
Viewing the table of tasks
Deleting a task from the list
Starting the tasks manually
Viewing task execution results
Configuring the storage time for the task execution results on the Administration Server
Managing Kaspersky Endpoint Agent activation tasks
Managing Kaspersky Endpoint Agent database update tasks
Creating Database and application module update task
Configuring Database and application module update task
Managing IOC Scan tasks in Kaspersky Endpoint Agent
About IOC Scan tasks in Kaspersky Endpoint Agent
Managing IOC Scan tasks in Kaspersky Endpoint Agent
Managing Standard IOC Scan tasks
Requirements for IOC files
Supported IOC terms
Creating and configuring Standard IOC Scan task
Configuring Standard IOC Scan task
IOC collection export
Viewing IOC Scan task execution results
Managing Autonomous IOC Scan tasks
About Autonomous IOC Scan tasks
Configuring user permissions to manage IOC Scan tasks
Configuring Autonomous IOC Scan task

IOC collection export
Viewing IOC Scan task execution results
Managing Kaspersky Endpoint Agent through command line interface
Managing Kaspersky Endpoint Agent activation
Configuring tracing
Configuring creation of dump files
Viewing information about quarantine settings and quarantined objects
Actions on quarantined objects
Managing Kaspersky Sandbox integration settings
Managing integration settings with KATA Central Node component
Running Kaspersky Endpoint Agent database and module update
Starting, stopping and viewing the current application status
Protecting the application with password
Protecting application services with PPL technology
Managing self-defense settings
Managing event filtering
Managing network isolation
Managing Standard IOC Scan tasks
Creating a backup copy and restoring the program from backup
Creating a backup copy of the program from the program administrator menu
Downloading a file containing a backup copy of the program from the Central Node or PCN server to the hard drive of the computer
Uploading a file containing a backup copy of the program from your computer to the Central Node server
Restoring the program from a backup copy through the program administrator menu
Creating a backup copy of the program in Technical Support Mode
Restoring the program from a backup copy in Technical Support Mode
Upgrading Kaspersky Anti Targeted Attack Platform
Installing program update packages in the administrator menu and in Technical Support Mode
Interaction with external systems via API
Interaction between an external system and Kaspersky Anti Targeted Attack Platform
Integrating an external system with Kaspersky Anti Targeted Attack Platform
API for scanning objects of external systems
Request to scan objects
Request for scan results
Request to delete scan results
Request to display object scan restrictions
API for sending alert information to external systems
Request to display alert information
Scope of transmitted data
Data on detected objects
Data on detected threats
Data on the environment of detected objects
Sources of information about the program
Contacting the Technical Support Service
How to obtain Technical Support
Technical Support via Kaspersky CompanyAccount

Glossary
- Advanced persistent threat (APT)
- Alternate data stream
- Anti-Malware Engine
- Backdoor program
- Central Node
- Communication channel bandwidth
- CSRF attack
- Distributed solution
- Dump
- End User License Agreement
- ICAP data
- Intrusion Detection System
- IOA
- IOC
- IOC file
- Kaspersky Anti Targeted Attack Platform
- Kaspersky Endpoint Agent
- Kaspersky Private Security Network
- Kaspersky Secure Mail Gateway
- Kaspersky Security Network (KSN)
- Kaspersky Threat Intelligence Portal
- KATA
- KEDR
- Local reputation database of KPSN
- Malicious web addresses
- Mirrored traffic
- MITM attack
- MITRE technique
- Multitenancy
- New generation threats
- NTP server
- OpenIOC
- Phishing URL addresses
- Sandbox
- Sensor
- SIEM system
- Signature
- SPAN
- Syslog
- TAA (IOA) rule
- Targeted attack
- Targeted Attack Analyzer
- TLS encryption
- Tracing
- VIP status
- YARA

YARA rules
Zero-day attack
Zero-day vulnerability
Information about third-party code
Trademark notices

# Kaspersky Anti Targeted Attack Platform Help

 What's new

 Hardware and software requirements

 Program architecture

 Program licensing

 Installation and initial configuration

- Standard Deployment Schemes
- Preparing for installing program components
- Procedure for installing program components
- Installation: Sandbox component
- Installing and configuring the Central Node and Sensor components
- Configuring integration with the Endpoint Agent component

 Upgrading the program

 Distributed solution

 Contacting the Technical Support Service

 API for interacting with external systems

 Sizing Guide

ksc_faq_discovering Managing the Sandbox component through the web interface

 Managing Kaspersky Endpoint Agent

 Working in the program web interface - For an administrator

- Monitoring program operation
- Managing accounts
- Managing Central Node, PCN, and SCN servers
- Managing the Sensor component
- Managing the Endpoint Agent component
- Integration with the Sandbox component
- Integration with external systems
- Integration with an SIEM system

 Working in the program web interface - For a security officer

- Monitoring program operation
- Filtering and searching alerts
- Events database threat hunting
- Tasks
- Policies
- User rules
- Storage and Quarantine
- Reports
- Object White List and exclusions for TAA and IDS rules
- Alerts with the VIP status
- Sending notifications about alerts and about program operation problems

# 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 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 Kaspersky Endpoint Agent and receive data from individual computers running Microsoft® Windows® OS in the corporate IT infrastructure. Kaspersky Endpoint Agent continuously monitors processes running, active network connections, and files that are being modified on those computers.
  - Kaspersky Endpoint Agent can be installed on individual computers and receive data from those computers.
  - Kaspersky Anti Targeted Attack Platform can be integrated with Kaspersky workstation protection programs (Endpoint Protection Platform (hereinafter also referred to as "EPP")): Kaspersky Endpoint Security for Windows, and Kaspersky Security for Windows Server.

    For detailed information about Kaspersky Endpoint Security for Windows and Kaspersky Security for Windows Server, see the online help of the relevant program.
- Integrate with external systems with the use of the REST API interface and scan files on these systems.

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, 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 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 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 information system known as Kaspersky Threat Intelligence Portal, which contains and displays information about the reputation of files and URLs.

- The Kaspersky Threats database.

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, view and manage each alert, and follow recommendations for evaluating and investigating incidents.

- Look through the table of events occurring on computers and servers of the corporate IT infrastructure, search for threats, filter, view and manage each event, follow recommendations for evaluating and investigating incidents.

- Run tasks on hosts with Kaspersky Endpoint Agent: run programs and stop processes, download and delete files, quarantine objects on Kaspersky Endpoint Agent workstations, place copies of files in Storage, and restore files from quarantine.

- Set up policies for preventing the running of files that they consider to be unsafe on selected hosts with Kaspersky Endpoint Agent.

- Isolate separate hosts with Kaspersky Endpoint Agent from the network.

- Work with TAA (IOA) rules to classify and analyze events.

- Manage user-defined Targeted Attack Analyzer TAA (IOA), Intrusion Detection System (IDS), and YARA rules — upload rules to be used for scanning objects and creating alerts.

- Work with OpenIOC compliant files (IOC files) to search for signs of targeted attacks, infected and probably infected objects on hosts with the Endpoint Agent component and in the Alerts database.
- Exclude TAA (IOA) rules and IDS rules defined by Kaspersky from scanning.
- Manage objects in quarantine and copies of objects in Storage.
- 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 TLS certificates and set up trusted connections between Central Node and Sandbox servers and between Kaspersky Anti Targeted Attack Platform servers and Kaspersky Endpoint Agent as well as external 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 experience.

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

# 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 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 website.

# Distribution kit

The Kaspersky Anti Targeted Attack Platform distribution kit includes the following files:

1. Disk image (file with the iso extension) containing the installation files for the CentOS 7.7 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 7.7 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. File with information about third-party code used in Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Agent distribution kit includes the following files:

Kaspersky Endpoint Agent distribution kit

| File | Description |
|---|---|
| `agent\endpointagent.msi` | Kaspersky Endpoint Agent installation package. |
| `agent\endpointagent.kud` | File for creating Kaspersky Endpoint Agent installation package using Kaspersky Security Center. |
| `agent\klcfginst.msi` | Installation package for Kaspersky Endpoint Agent Management plug-in for Kaspersky Security Center. |
| `agent\kpd.loc\en-us.ini` | Configuration file required for creating installation package for English version of Kaspersky Endpoint Agent using Kaspersky Security Center. |
| `agent\kpd.loc\ru-ru.ini` | Configuration file required for creating installation package for Russian version of Kaspersky Endpoint Agent using Kaspersky Security Center. |
| `agent\en-us\ksn.txt` | File with the text of the terms of participation in Kaspersky Security Network in English. |
| `agent\en-us\license.txt` | File with the text of the End User License Agreement and the Privacy Policy in English. |
| `agent\en-us\release_notes.txt` | File with the text of the Release Notes for Kaspersky Endpoint Agent in English. |
| `agent\ru-ru\ksn.txt` | File with the text of the terms of participation in Kaspersky Security Network in Russian. |

| File | Description |
| --- | --- |
| `agent\ru-ru\license.txt` | File with the text of the End User License Agreement and the Privacy Policy in Russian. |
| `agent\ru-ru\release_notes.txt` | File with the text of the Release Notes for Kaspersky Endpoint Agent in Russian. |

# 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 80 or later.
- Google Chrome for Linux version 80 or later.
- Mozilla™ Firefox™ version 73 or later.
- Microsoft Edge 80 or later.
- Safari 13.0 or later.

Minimum screen resolution to use web interface: 1366x768.

Deploying the program on a virtual platform requires installing the VMware ESXi™ 6.5.0 or 6.7.0 hypervisor.

The configuration of the servers hosting the Central Node, Sandbox and Sensor components depends on the volume of data processed by the program and the bandwidth of the communication channel.

For the Central Node, Sensor and Sandbox hardware requirements see the Sizing Guide.

# Requirements for Kaspersky Endpoint Agent

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

If the version of Kaspersky Anti Targeted Attack Platform program on Central Node servers is incompatible with the version of Kaspersky Endpoint Agent (previously known as Endpoint Sensors) installed on corporate LAN computers, the functionality of Kaspersky Anti Targeted Attack Platform can be limited: IOC scanner on computers with Kaspersky Endpoint Agent as well as managing tasks and policies created on computers with Kaspersky Endpoint Agent can be unavailable from Central Node servers.

## Software requirements for installing Kaspersky Endpoint Agent

Kaspersky Endpoint Agent only works on computers that have one of the following operating systems installed:

- Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit
- Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit
- Windows 10 RS3 (version 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS4 (version 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 (version 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS6 (version 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 (version 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2012 Foundation / Standard / Enterprise 64-bit
- Windows Server 2012 R2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit
- Windows Server 2019 Essentials / Standard / Datacenter 64-bit

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

Kaspersky Endpoint Security including Endpoint Sensors component version 3.6.1 supports fewer operating systems than KES version 11.2 without a built-in Endpoint Sensors program.

To use Kaspersky Endpoint Agent with Kaspersky Security for Virtualization Light Agent in a 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.
- Citrix Hypervisor platform: Citrix XenServer 7.1 LTSR hypervisor.
- VMware vSphere platform:
  - VMware ESXi 6.7 hypervisor
  - VMware ESXi 6.5 hypervisor

- 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.

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

- Endpoint Sensors version 3.6.1 forms part of KES version 11.2.
- Endpoint Sensors version 3.6 forms part of KES version 11.1.1.
- Endpoint Sensors version 3.0 forms part of KES version 10 SP2 MR3 and 11.0.

### Hardware requirements for installing Kaspersky Endpoint Agent

Minimum configuration:

- CPU: 1.4 GHz (single core) or higher.
- RAM: 256 MB (512 MB for a 64-bit operating system).
- Available disk space: 500 MB.
- One network adapter with a data transfer speed of 1 Gbit/s.

When integrated with the Kaspersky 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 Kaspersky Endpoint Agent (Endpoint Sensors) versions with Kaspersky Anti Targeted Attack Platform versions

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

If the version of the program installed on Central Node servers is incompatible with the version of Kaspersky Endpoint Agent installed on computers on the corporate LAN, the functionality of Kaspersky Anti Targeted Attack Platform may be limited. For example, IOC scanning of files and working with created tasks and policies on computers with Kaspersky Endpoint Agent can be unavailable for Central Node servers.

Information about the compatibility of Kaspersky Endpoint Agent (Endpoint Sensors) component versions with Kaspersky Anti Targeted Attack Platform versions is listed in the table below.

Compatibility of Kaspersky Endpoint Agent (Endpoint Sensors) versions with Kaspersky Anti Targeted Attack Platform versions

| Version of Endpoint Agent (Endpoint Sensors) | Type of Endpoint Agent (Endpoint Sensors) | Compatibility with KATA 3.5 | Compatibility with KATA 3.6 | Compatibility with KATA 3.6.1 | Compatibility with KATA 3.7 | Compatibility with KATA 3.7.1 |
|---|---|---|---|---|---|---|
| Endpoint Sensors 3.1.406 | Installed as part of KES version 11.0 | Available functionality:<br>• Monitoring<br>• Alerts<br>• Events<br>• Tasks (only **Restore file from Quarantine**). | Available functionality:<br>• Monitoring<br>• Alerts<br>• Events<br>• Tasks (only **Restore file from Quarantine**). | Available functionality:<br>• Monitoring<br>• Alerts<br>• Events<br>• Tasks (only **Restore file from Quarantine**). | No | No |
| Endpoint Sensors 3.5.X | Standalone installation or part of KES version 11.1 | Yes | Yes | Yes | Available functionality:<br>• Monitoring<br>• Alerts (only TAA) | Available functionality:<br>• Monitoring<br>• Alerts (only TAA) |
| Endpoint Sensors 3.6 | Standalone installation or part of KES version 11.1.1 | No | Yes | Yes | Available functionality:<br>• Monitoring<br>• Alerts (only TAA) | Available functionality:<br>• Monitoring<br>• Alerts (only TAA) |
| Endpoint Sensors 3.6.1 | Standalone installation or part of KES versions 11.2 and 11.3 | No | No | Yes | Available functionality:<br>• Monitoring<br>• Alerts (only TAA) | Available functionality:<br>• Monitoring<br>• Alerts (only TAA) |
| Endpoint Agent 3.8 | Standalone installation | No | No | No | Yes | Yes |
| Endpoint Agent 3.9 | Standalone installation or part of KES version 11.4 and 11.5 | No | No | No | Yes | Yes |
| Endpoint Agent 3.10 | Standalone installation or part of KES version 11.6 | No | No | No | No | Yes |

If you are using both Endpoint Sensors 3.6.X installed as part of Kaspersky Endpoint Security and the standalone Kaspersky Endpoint Agent 3.8 or 3.9 simultaneously, Kaspersky Anti Targeted Attack Platform receives data from both programs. The following errors can result from this:

- Information about IDS and Sandbox alerts is not received from Endpoint Sensors 3.6.X.
- Kaspersky Endpoint Agent 3.8 or 3.9 does not send alert information to Kaspersky Endpoint Security

*To avoid the errors, do one of the following:*

- Disable the use of Kaspersky Endpoint Agent program as part of Kaspersky Endpoint Security before upgrading Kaspersky Endpoint Agent program to version 3.8 or 3.9.
- Before and after upgrading Kaspersky Endpoint Agent to version 3.8 or 3.9, disable the use of version 3.6.X in Kaspersky Endpoint Agent program policy.

# Compatibility of the Kaspersky Endpoint Agent (Endpoint Sensors) component versions with Kaspersky Endpoint Security versions

You can install Kaspersky Endpoint Agent (Endpoint Sensors) as part of Kaspersky Endpoint Security or separately.

When Kaspersky Endpoint Agent (Endpoint Sensors) is installed as part of Kaspersky Endpoint Security, the programs integrate with each other. In this case, Kaspersky Endpoint Agent also sends information about threats detected by Kaspersky Endpoint Security and results of threat processing by this program to the Central Node server.

You can install the following versions of Kaspersky Endpoint Agent (Endpoint Sensors) as part of Kaspersky Endpoint Security:

- Kaspersky Endpoint Agent 3.7 or Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 as part of Kaspersky Endpoint Security 11.2, 11.3.

  Kaspersky Endpoint Agent 3.7 is incompatible with Kaspersky Anti Targeted Attack Platform.

- Kaspersky Endpoint Agent 3.9 as part of Kaspersky Endpoint Security 11.4, 11.5.

- Kaspersky Endpoint Agent 3.10 as part of Kaspersky Endpoint Security 11.6.

When you install Kaspersky Endpoint Agent (Endpoint Sensors) as part of Kaspersky Endpoint Security, the standalone Kaspersky Endpoint Agent (Endpoint Sensors) program of the same or earlier version is removed.

Information about the compatibility of Kaspersky Endpoint Agent (Endpoint Sensors) versions with Kaspersky Endpoint Security versions is listed in the table below.

Compatibility of the Kaspersky Endpoint Agent (Endpoint Sensors) versions with Kaspersky Endpoint Security versions

| Kaspersky Endpoint Security version | Compatibility with Endpoint Sensors 3.6 and 3.6.1 | Compatibility with Endpoint Agent 3.8 | Compatibility with Endpoint Agent 3.9 | Compatibility with Endpoint Agent 3.10 |
|---|---|---|---|---|
| • KES 10 SP2 MR2 | Yes | No | No | No |
| • KES 10 SP2 MR3/MR4 | Yes | Yes | Yes | No |
| • KES 11.0.0 | Yes | No | No | No |
| • KES 11.0.1 | Yes | Yes | Yes | No |
| • KES 11.1<br>• KES 11.1.1 | No | Yes | Yes | Yes |
| • KES 11.2<br>• KES 11.3 | Yes | Yes | Yes | Yes |
| • KES 11.4 | No | Yes | Yes | Yes |
| • KES 11.5 | No | Yes | Yes | Yes |
| • KES 11.6 | No | Yes | Yes | Yes |

If you are using both Endpoint Sensors 3.6.X installed as part of Kaspersky Endpoint Security and the standalone Kaspersky Endpoint Agent 3.8 or 3.9 simultaneously, Kaspersky Anti Targeted Attack Platform receives data from both programs. The following errors can result from this:

- Information about IDS and Sandbox alerts is not received from Endpoint Sensors 3.6.X.
- Kaspersky Endpoint Agent 3.8 or 3.9 does not send alert information to Kaspersky Endpoint Security

*To avoid the errors, do one of the following:*

- Disable the use of Kaspersky Endpoint Agent program as part of Kaspersky Endpoint Security before upgrading Kaspersky Endpoint Agent program to version 3.8 or 3.9.
- Before and after upgrading Kaspersky Endpoint Agent to version 3.8 or 3.9, disable the use of version 3.6.X in Kaspersky Endpoint Agent program policy.

You can upgrade Kaspersky Endpoint Agent to versions 3.8 and 3.9 either as part of Kaspersky Endpoint Security or separately. When you upgrade Kaspersky Endpoint Agent as part of Kaspersky Endpoint Security, the integration of compatible program versions is maintained. You can upgrade a previous version of Kaspersky Endpoint Agent to version 3.10 only for Kaspersky Endpoint Agent versions 3.8 and 3.9.

# Compatibility of Kaspersky Endpoint Agent with other programs

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

## Compatibility of Endpoint Sensors 3.5 with Kaspersky programs

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

1. Disable Endpoint Sensors in the KES program.

   For details on how to disable Endpoint Sensors in the KES program, refer to the *Kaspersky Endpoint Security Help*.

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

## Compatibility of Endpoint Sensors 3.6 with Kaspersky Endpoint Security for Windows

Information about the compatibility of Endpoint Sensors 3.6 with Kaspersky Endpoint Security for Windows (hereinafter also referred to as "KES") is listed in the following table.

Kaspersky Endpoint Security version 11.1.1 is compatible only with the Endpoint Sensors program that is part of KES. You cannot install KES 11.1.1 and the standalone Endpoint Sensors program on the same computer.

Compatibility of Endpoint Sensors with KES.

| Version of the Kaspersky program | Compatibility mode | Installing the standalone Endpoint Sensors program after installing the other program | Installing the other program after installing the standalone Endpoint Sensors program | Supported operating systems |
|---|---|---|---|---|
| • KES10 SP1 MR3 (Endpoint Sensors as part of KES version 1.0)<br>• KES10 SP1 MR4 (Endpoint Sensors as part of KES version 1.0) | Joint operation.<br>Using Endpoint Sensors as part of KES is **not supported**. | Standard installation procedure. | KES when installed over the stand-alone Endpoint Sensors program **does not remove** the stand-alone Endpoint Sensors program. | • Windows 7 SP1 Enterprise x86 x64<br>• Windows 8.1.1 Enterprise x86 x64.<br>• Windows 10 RS3 Enterprise x86 x64<br>• Windows 10 RS4 Enterprise x86 x64<br>• Windows 10 RS5 Enterprise x86 x64<br>• Windows 10 RS6 Enterprise x86 x64<br>• Windows Server 2008 R2 Enterprise x64.<br>• Windows Server 2012 Standard x64.<br>• Windows Server 2012 R2 Standard x64.<br>• Windows Server 2016 Standard x64. |
| • KES 10 SP2 (Endpoint Sensors as part of KES version 2.0)<br>• KES 10 SP2 MR1 (Endpoint Sensors as part of KES version 2.0)<br>• KES 10 SP2 MR2 (Endpoint Sensors as part of KES version 2.0) | Joint operation.<br>Using Endpoint Sensors as part of KES is **not supported**. | Standard installation procedure. | KES when installed over the stand-alone Endpoint Sensors program **does not remove** the stand-alone Endpoint Sensors program. | |
| • KES 10 SP2 MR3 (Endpoint Sensors as part of KES version 2.0) | Joint operation.<br>Using Endpoint Sensors as part of KES **is supported**. | Standard installation procedure. | KES when installed over the stand-alone Endpoint Sensors program **does not remove** the stand-alone Endpoint Sensors program. | |
| • KES 11.0.0 (Endpoint Sensors as part of KES version 3.0) | Joint operation.<br>Using Endpoint Sensors as part of KES is **not supported**. | To install the standalone Endpoint Sensors program, the Endpoint Sensors built into the KES program must be disabled.<br>For details on how to disable Endpoint Sensors in the KES program, refer to the *Kaspersky Endpoint Security Help*.<br>If the program is not disabled, installation fails with an error. | KES when installed over the stand-alone Endpoint Sensors program **does not remove** the stand-alone Endpoint Sensors program regardless of whether an Endpoint Sensors program is included with the KES program. | |
| • KES 11.0.1 (Endpoint Sensors as part of KES version 3.0) | Joint operation.<br>Using Endpoint Sensors as part of KES **is supported**. | To install the standalone Endpoint Sensors program, the Endpoint Sensors built into the KES program must be disabled.<br>For details on how to disable Endpoint Sensors in the KES program, refer to the *Kaspersky Endpoint Security Help*.<br>If the program is not disabled, installation fails with an error. | KES when installed over the stand-alone Endpoint Sensors program **does not remove** the stand-alone Endpoint Sensors program regardless of whether an Endpoint Sensors program is included with the KES program. | |
| • KES 11.1 (Endpoint Sensors as part of KES version 3.5) | Joint operation is not supported.<br>Only the built-in Endpoint Sensors program as part of KES can be used. | A stand-alone Endpoint Sensors program cannot be installed over KES.<br>You can enable the built-in Endpoint Sensors program as part of the KES program. | KES **removes** the standalone Endpoint Sensors program.<br>Settings of the stand-alone Endpoint Sensors program are not preserved. | |

## Compatibility of Endpoint Sensors version 3.6 with Kaspersky Security for Windows Server version 10.1.2 (KSWS 10.1.2)

Installing the Endpoint Sensors program version 3.6.0.62 on the same server as the KSWS application version 10.1.2 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.

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

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

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

To use Endpoint Sensors with KSV LA 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.
- Citrix Hypervisor platform: Citrix XenServer 7.1 LTSR hypervisor.
- VMware vSphere™ platform:
  - VMware ESXi 6.7 hypervisor
  - VMware ESXi 6.5 hypervisor
- 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.

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

## Compatibility of Kaspersky Endpoint Agent 3.8 with Kaspersky Security for Virtualization Light Agent (KSV LA)

Kaspersky Endpoint Agent 3.8 is compatible with Kaspersky Security for Virtualization Light Agent (KSV LA) versions 5.1, 5.1.1, 5.1.2, 5.1.3.

## Compatibility of Kaspersky Endpoint Agent versions 3.8 and 3.9 with Kaspersky Endpoint Protection Platform programs

Kaspersky Endpoint Agent versions 3.8 and 3.9 are compatible with the following Endpoint Protection Platform programs:

- Kaspersky Endpoint Security 10 for Windows: 10 SP2 MR3, 10 SP2 MR4.
- Kaspersky Endpoint Security 11 for Windows: 11.0.1, 11.1, 11.1.1, 11.2, 11.3, 11.4, 11.5, 11.6.
- Kaspersky Security 10 for Windows Server: 10.1.2, 11.

If Endpoint Sensor version 3.6.X is installed and used on the device as part of Kaspersky Endpoint Security, it is recommended to disable Endpoint Sensor before installing Kaspersky Endpoint Agent 3.8 and 3.9 to avoid possible conflicts between the programs.

## Compatibility of Kaspersky Endpoint Agent program versions 3.8 and 3.9 with other Kaspersky programs

Kaspersky Endpoint Agent program versions 3.8 and 3.9 are compatible with the following Kaspersky programs and solutions:

- Kaspersky Security Center 11, 12, and later.
- Kaspersky Sandbox 1.0.
- Kaspersky Anti Targeted Attack Platform 3.7, 3.7.1, 3.7.2.

## Compatibility of Kaspersky Endpoint Agent 3.10 with programs of Kaspersky Endpoint Protection Platform

Kaspersky Endpoint Agent versions 3.10 is compatible with the following Endpoint Protection Platform programs:

- Kaspersky Endpoint Security 11 for Windows: 11.1.1, 11.2, 11.3, 11.4, 11.5, 11.6.
- Kaspersky Security 10 for Windows Server: 10.1.2.
- Kaspersky Security 11 for Windows Server.

## Kaspersky Endpoint Agent 3.10 compatibility with other Kaspersky applications

Kaspersky Endpoint Agent 3.10 is compatible with the following Kaspersky applications and solutions:

- Kaspersky Security Center versions 11 and 12.1.
- Kaspersky Security Center Cloud Console.
- Kaspersky Sandbox 1.0.
- Kaspersky Anti Targeted Attack Platform 3.7.1, 3.7.2.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

For information about managing Kaspersky Endpoint Agent 3.10 refer to the *Kaspersky Endpoint Agent 3.10 Help*.

## Compatibility of the Kaspersky Endpoint Agent program with third-party antivirus programs

One of the following third-party anti-virus programs can be installed on computers on which you want to install Kaspersky Endpoint Agent (Endpoint Sensors):

- Symantec™ Endpoint Protection.
- Trend Micro™ Maximum Security.
- Sophos Endpoint Protection.
- ESET NOD32 Business Edition Smart Security.
- BitDefender GravityZone Advanced Business Security.
- McAfee® Endpoint Security 10.6.1.

If you install more than one third-party anti-virus program, correct operation of Kaspersky Endpoint Agent (Endpoint Sensors) is not guaranteed.

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

# Limitations of the current version of the program

## Kaspersky Anti Targeted Attack Platform 3.7.1 has the following known limitations:

1. To install the 3.7.1 upgrade package, you must use the administrator menu or the Tech Support Mode.

## Kaspersky Endpoint Agent 3.8 has the following known limitations:

1. You can install Kaspersky Endpoint Agent through Kaspersky Security Center (KSC) or locally on computers of your corporate LAN. If you are installing Kaspersky Endpoint Agent locally, keep in mind that the installation wizard does not support user names containing CJK characters. To install Kaspersky Endpoint Agent on computers of users whose names contain CJK characters, you must use KSC.

2. If Kaspersky Endpoint Agent is used on the same device with Kaspersky Endpoint Security, and the file system level encryption (FLE) component is installed in Kaspersky Endpoint Security, Kaspersky Endpoint Agent does not register telemetry events about loading modules (LoadImage) and does not send these events to KATA Central Node component.

3. When scanning for indicators of compromise, if the search involves parsing text strings, the "is" condition takes into account whitespace, and the need to escape the indicator description in the IOC file with CDATA characters. For example, to detect an object with the copyright "Copyright (C) 1998-2017 Mark Russinovich" by the "is" condition, the indicator description must be specified in the following format: <Content type="string"><![CDATA[Copyright (C) 1998-2017 Mark Russinovich ]]></Content>.

   To simplify description of the indicators, the “contains” condition can also be used.

4. Kaspersky Endpoint Agent can double-display data about a triggered object when displaying the results of IOC Scan task.

5. The installer cannot stop the soyuz service until the service is initialized. For example, the installer returns the "Invalid password" error when trying to remove or modify the configuration of the application immediately after installation is completed, since initialization of the soyuz service is not completed and the service cannot be stopped.

6. When scanning objects using the FileItem IOC document, Kaspersky Endpoint Agent skips objects with restricted access, for example, files that are used by other applications at the time of scanning. Kaspersky Endpoint Agent returns a false negative scan result for such objects.

7. If localization of Kaspersky Endpoint Agent differs from localization of Kaspersky Endpoint Agent management plug-in for Kaspersky Security Center, some settings may be displayed incorrectly in the output of commands with the “show" option to the command console.

8. When searching for indicators in the modules loaded into the address space, Kaspersky Endpoint Agent skips cases when the system loads x64 modules into x32 processes. For example, the following cases will not be detected: loading wowcpu64.dll into system32 or loading ntdll into system32. This limitation is reproduced in Windows Server 2008 R2 and Windows 7 x64 operating systems.

9. When trying to launch Kaspersky Endpoint Agent installer with the permissions of a user whose account contains Chinese characters, the installer fails. It is recommended to install the application with the Local System account permissions, for example, start installation using Kaspersky Security Center.

10. Kaspersky Endpoint Agent 3.8 cannot be restored or uninstalled from the device if the integrity of the agent.exe module (Kaspersky Endpoint Agent 3.8 command line utility) is violated.

11. The capability to run and execute Kaspersky Endpoint Agent service (soyuz.exe) with the PPL flag is implemented. This feature is provided by the klelaml.sys driver. Violation of the klelaml.sys driver integrity results in the operating system loading failure. In this case, it is recommended to use Windows system recovery utilities. The absence of the klelaml.sys driver when the PPL flag is enabled for the soyuz.exe process does not lead to the operating system failure, but results in Kaspersky Endpoint Agent crash. In this case, it is recommended to run the application installer and perform recovery in the quiet mode with the REINSTALL=Drivers.klelam key.

12. Kaspersky Endpoint Agent installer cannot be launched on a device with the operating system to which the active CodeIntegrity policy is applied.

13. In Kaspersky Endpoint Agent properties in the Administration Console (in the General section), data about the application installation status is displayed incorrectly.

14. Objects quarantined by Kaspersky Endpoint Agent cannot be sent from Kaspersky Security Center quarantine to Kaspersky for analysis.

15. When the active policy sections are deactivated, the "Kaspersky Security Center policy is activated" (5) event is generated instead of the "Kaspersky Security Center policy is deactivated" (7) event.

16. The check boxes corresponding to the Read and Perform operations with device selections permissions that are displayed in the group of settings for role-based access control (RBAC) in the Administration Console, in the section with permissions for managing Kaspersky Endpoint Agent plug-in, do not apply to the group of settings in Kaspersky Security Center. If you select these check boxes, the Read and Perform operations with device selections permissions will not be restricted for the specified users.

17. When generating event selections, the filters are not applied to some of Kaspersky Endpoint Agent events published in Kaspersky Security Center Administration Console.

18. Cosmetic errors in the application interface have not been fixed, such as trimmed text in the control interface.

19. The agent.exe --help command does not support output of help for one specified command. The full list of all commands supported by the utility is displayed in the console.

20. The name of the workgroup, but not the name of the user is displayed in the User field in the properties of the object quarantined to the Administration Server repository.

21. The agent.exe command line utility does not support operation with Cyrillic characters. For example, if a node whose address contains Cyrillic characters is specified in the list of Kaspersky Sandbox nodes in Kaspersky Endpoint Agent settings, the output of the --sandbox=show command may contain errors.

22. The installer of Kaspersky Endpoint Agent and Kaspersky Endpoint Agent management plug-in automatically selects the application localization based on the operating system regional settings on the device where the application or management plug-in is installed:

    - if the operating system uses the RU-RU locale, the Russian version of Kaspersky Endpoint Agent and Kaspersky Endpoint Agent management plug-in is installed;

    - if the operating system uses any locale other than RU-RU, the English version of Kaspersky Endpoint Agent and Kaspersky Endpoint Agent management plug-in is installed.

23. Application localization affects the language of texts used to describe application modules in the system and when publishing application events to the Windows Event Log, as well as texts of Kaspersky Security Center reports. Kaspersky Endpoint Agent management plug-in localization affects the language of texts used in the application interface of Administration Console (interface of policies, group tasks, and application properties). The application localization cannot be configured manually.

    Please note that if regional settings on managed devices and on the device with Kaspersky Endpoint Agent management plug-in do not match, localization of Kaspersky Endpoint Agent interface in the Administration Console and localization of events published by the application in Kaspersky Security Center reports may not match. Also, the localization of the application interface in the Administration Console and the localization of events published by the application in Kaspersky Security Center reports may differ from the localization of Administration Console interface and the compatible EPP interface in the Administration Console.

24. Kaspersky Endpoint Agent saves objects to a queue before sending them to Kaspersky Sandbox for scan. The path to the queue folder can be configured in the application policy. By default, Kaspersky Endpoint Agent uses the %APPDATA%\Sandbox\Queue folder.

    In order to prevent integration errors with Kaspersky Sandbox, consider the following recommendations:

    - When changing the default settings, make sure that the folder you specify exists.

    - When changing the default settings, make sure that the Local System user has at least write permissions to the specified folder.

    - Do not delete the folder used for the queue. Do not change the attributes of this folder.

25. To perform an automatic IOC Scan task in the policy or in the application properties, the login credentials for the Administration Server with write and execute permissions must be specified. If this data is not specified, Kaspersky Endpoint Agent cannot automatically create group IOC Scan tasks.

# About data provision

The operation of certain components of Kaspersky Anti Targeted Attack Platform requires data processing on the Kaspersky 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:

- 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 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. 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, they are accumulated in the cache on servers hosting Kaspersky Anti Targeted Attack Platform components.

Kaspersky protects any information received in this way as prescribed by law and applicable rules of Kaspersky. Data is sent over encrypted communication channels.

When using Kaspersky Private Security Network, Kaspersky 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

# Traffic data of the Sensor component

Traffic data of the Sensor component is stored on the server with the Sensor component or on the server with Sensor and Central Node components if Sensor and Central Node are installed on the same server.

Traffic data is recorded and stored in sequentially created files. The program stops recording data in one file and starts logging data in the next file if:

- The maximum file size is reached (you can configure this setting)
- The configured time interval has elapsed (you can configure this setting)
- The traffic saving service or the entire Kaspersky Anti Targeted Attack Platform program is restarted

As traffic data accrues, Kaspersky Anti Targeted Attack Platform filters data and keeps only the following information:

- Information related to alerts generated by the Targeted Attack Analyzer technology
- PCAP files in which:
  - Source or destination IP address matches an IP address from the alert
  - Traffic data belongs to the time period within 15 minutes from the alert time

Filtered traffic data is moved to a separate section. The rest of the traffic data (that do not satisfy filtering criteria) is deleted.

Filtered traffic data is saved in sequentially created files. The program stops recording data in one file and starts logging data in the next file if:

- The maximum file size is reached
- The configured time interval has elapsed

Filtered data traffic is stored for the last 24 hours. Older data is deleted.

# 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 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 that were 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 Agent component (previously known as Endpoint Sensors): IP address, name, domain of the host (in FQDN format), full path to the file on the computer with the Endpoint Agent 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 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 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 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 can be stored on the server:

- Version of YARA rules that was 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 by IOC or TAA (IOA) user rules, the following information can 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 can contain information related to the following:

- Name of the computer where the event occurred.
- Name of the user account under which the event occurred.
- Unique ID of the computer with Kaspersky Endpoint Agent (previously known as Endpoint Sensors).
- Event type.
- Event time.
- Full paths to files on computers with Kaspersky Endpoint Agent.
- Names of files on computers with Kaspersky Endpoint Agent.
- Full names of folders on computers with Kaspersky Endpoint Agent.
- 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 Kaspersky Endpoint Security 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.

# 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 Storage and Quarantine

Objects in Storage and Quarantine may contain user data. Information about objects in Storage and about copies of objects quarantined on computers with Kaspersky Endpoint Agent using the **Get file** tasks is stored indefinitely on the Central Node server in the /data/var/lib/kaspersky/storage/pgsql/10/data/ directory.

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 Storage and Quarantine may contain the following information:

- Name of the object.
- Path to the object on the computer with Kaspersky Endpoint Agent (previously known as Endpoint Sensors).
- MD5- and SHA256 hash of the file.
- ID of the user who quarantined the object on the computer with Kaspersky Endpoint Agent (previously known as Endpoint Sensors).
- ID of the user who placed the object in Storage.
- Unique ID of the computer on which the quarantined object is stored in Storage.

- Category of the detected object.
- Results for the object scanned using individual modules and technologies of the program.

# 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.

## Information about Endpoint Agent components (previously known as Endpoint Sensors)

Information about Endpoint Agent components may contain the following:

- Unique ID of the computer with the Endpoint Agent component.
- Name of the computer with the Endpoint Agent 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 Agent component.
- Time and result of the last IOC scan on the computer with the Endpoint Agent component.

## Information about parameters of IOC and TAA (IOA) user rules.

Information about parameters of IOC and TAA (IOA) user rules can contain the following:

- Name of the IOC file.
- Requests to scan using IOC and TAA (IOA) user rules.
- Time of last scan completion.
- State of the IOC file.
- Date when the IOC file was loaded.
- Importance level of generated alerts.

## Information about parameters of IDS user rules

Information about parameters of IDS user rules can contain the following:

- Name of the imported IDS rule.
- Requests to scan using the IDS rule.
- Time of last scan completion.
- State of the user rule file.
- Import date of the user rule file.
- 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 Agent 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.

Service data necessary for program operation

| Data type | Storage location | Access to data | Storage duration |
|---|---|---|---|
| Event log of the operating system. | • /var/log | Access for users with root privileges. | Indefinite. |
| Program data cache (redis). | • /var/log | User access is defined by the administrator using operating system tools.<br>Access is provided only over an encrypted IPSec channel. | Indefinite. |
| Alert export files.<br>Files may contain the following information:<br>• Name of the computer on which the alert was generated.<br>• Alert time.<br>• Category of the detected object.<br>• IP address of the data packet sender.<br>• IP address of the data packet recipient.<br>• URL address of the data packet sender.<br>• URL address of the data packet recipient.<br>• UserAgent of the computer with the Endpoint Agent component.<br>• URL of the visited website.<br>• MD5 hash of the detected object.<br>• SHA256 hash of the detected object.<br>• Full name of the detected object.<br>• Command-line parameters.<br>• Email address of the sender of the message in which the object was detected.<br>• Email addresses of the recipients of the message in which the object was detected.<br>• Name of the domain in which the alert was generated. | • /var/log | User access is defined by the administrator using operating system tools.<br>Data export is available only for authorized users.<br>Access is provided only over an encrypted IPSec channel. | Indefinite. |
| Artifacts of the Sandbox component, PCAP files of intercepted traffic. | • /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. | • /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 Agent component. | • /var/opt/kaspersky/apt/edr_quarantine<br>• /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 | • /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. | • /etc/ssl/certs | User access is defined by the administrator using operating system tools.<br>Information about actions with certificates is saved in the program event log. | Indefinite. |
| Encryption keys transmitted between program components. | • /etc/opt/kaspersky/apt-base/ipsec.d | User access is defined by the administrator using operating system tools. | Indefinite. |

| Data type | Storage location | Access to data | Storage duration |
|---|---|---|---|
| | | Information about modifications to encryption keys is saved in the program event log. | |

# 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.

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 | • /var/opt/kaspersky/sandbox/library/<br>• /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 | • /var/opt/kaspersky/sandbox/library/<br>• Sandbox component database | 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/.<br>Up to 90 days in the Sandbox component database. | User access to the directory /var/opt/kaspersky/sandbox/library/ is defined by the administrator using operating system tools.<br>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.<br>Access is provided only over an encrypted IPSec channel. |
| Trace files | /var/log/kaspersky/sandbox/ | Up to 21 days. | User access is defined by the administrator using operating system tools.<br>Only authorized users can perform actions with trace files.<br>Information about actions with trace files is saved in the program event log. |

# Data transmitted between program components

## Central Node and Kaspersky Endpoint Agent (previously known as Endpoint Sensors)

Kaspersky Endpoint Agent sends the following to the Central Node component: task completion reports, information on events and alerts that occurred on computers with Kaspersky Endpoint Agent, and information on terminal 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 Kaspersky Endpoint Agent is removed from the computer, but no longer than 21 days.

If an event occurred on the user's computer, Kaspersky Endpoint Agent 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, PriviledgeList, 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 program, if integration with a proxy server 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 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 scans using IOC, TAA (IOA), IDS, YARA user rules.
- Data on files in Storage.
- Data on user accounts.

- Data on the license.
- List of computers with Kaspersky Endpoint Agent installed
- Objects placed in Storage.
- Objects quarantined on computers with Kaspersky Endpoint Agent.
- Files attached to alerts.
- IOC files.

# Data of Kaspersky Endpoint Agent

Kaspersky Endpoint Agent stores and processes data locally to provide base functionality and audit capability, as well as to improve the speed with which Kaspersky Technical Support can solve potential problems.

Computers with Kaspersky Endpoint Agent store data prepared to be sent automatically to Kaspersky Anti Targeted Attack Platform servers and Kaspersky Security Center.

Files prepared by Kaspersky Endpoint Agent to be sent for scanning to program servers are stored on computers with Kaspersky Endpoint Agent in plain unencrypted form in the directory that is used by default for storing files prior to sending them.

Files associated with detected events can 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 Kaspersky Endpoint Agent to the server with the Central Node component cannot be disabled.

Do not use Kaspersky Endpoint Agent on computers from which data transfer is forbidden by your corporate policy.

Data received from Kaspersky Endpoint Agent 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 Kaspersky Endpoint Agent to the server with the Central Node component are stored on computers hosting Kaspersky Endpoint Agent in plain unencrypted 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 Kaspersky Endpoint Agent are only sent to the server with the Central Node component over a secure SSL connection.

Files that have been encrypted on computers with the Endpoint Agent 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 Kaspersky Endpoint Agent that impact the performance of the computer during interaction with the Central Node component.

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

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

The Kaspersky Anti Targeted Attack Platform administrator must take steps to ensure the security of computers with Kaspersky Endpoint Agent and Kaspersky Anti Targeted Attack Platform servers with the data listed above. 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 Kaspersky Endpoint Agent:

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

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

# Data received from the Central Node component

Kaspersky Endpoint Agent 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 Agent\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. Kaspersky Endpoint Agent component does not manage access permissions to this folder and any files in it. It is the system administrator who determines access permissions.

Data is deleted when Kaspersky Endpoint Agent 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 Kaspersky Endpoint Agent.
- 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 Kaspersky Endpoint Agent.
- Names of files on computers with Kaspersky Endpoint Agent.
- Masks of files on computers with Kaspersky Endpoint Agent.
- Full names of folders on computers with Kaspersky Endpoint Agent.
- 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 fields of Windows Event Log events of Kaspersky Endpoint Agent

Windows Event Log data is stored in the %SystemRoot%\System32\Winevt\Logs\Kaspersky-Security-Soyuz%4Product.evtx file in plain unencrypted form. The data is stored until Kaspersky Endpoint Agent is uninstalled.

The data can be sent to Kaspersky Security Center automatically, but is not sent to Kaspersky Sandbox.

By default, only users with System and Administrator permissions have read-access to the files. Kaspersky Endpoint Agent does not manage access permissions to this folder and the files in this folder. It is the system administrator who determines access permissions.

Event data can contain information related to the following:

- Data on user sessions in the operating system.
- Operating system user accounts (userID).
- Errors occurred during object scan tasks execution.

- Object scanning tasks.
- Kaspersky Sandbox alerts.
- Kaspersky Sandbox events.
- Kaspersky Endpoint Agent IOC files generated as part of automatic Threat Response.
- Object scan results.
- Kaspersky Sandbox server certificates.
- The object scan queue.
- Modified settings of Kaspersky Endpoint Agent.
- Changes of Kaspersky Security Center policies.
- Modified status of an object scan task.
- Kaspersky Security Center policies.
- Quarantined objects.
- Automatic Threat Response actions.
- Errors of interaction with program servers.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

# Data in Kaspersky Endpoint Agent requests to Kaspersky Anti Targeted Attack Platform

When integrated with the Central Node component, the following data is stored locally on the device with Kaspersky Endpoint Agent installed.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Data from Kaspersky Endpoint Agent requests to the Central Node component:

1. In the synchronization requests:
   - Unique Kaspersky Endpoint Agent identifier.
   - Basic part of the server web address.
   - Device name.

- Local time on the device.
- Self-defense status of Kaspersky Endpoint Agent.
- Name and version of the operating system that is installed on the device.
- Kaspersky Endpoint Agent version.
- Versions of the application settings and task settings.
- Task statuses in Kaspersky Endpoint Agent: identifiers of running tasks, execution statuses, execution error codes.
- Statuses of Kaspersky Endpoint Agent settings: type of settings being used, version of settings, status of applying the settings, error codes of applying the settings.

2. In requests for obtaining files from the server:

- Unique identifiers of files.
- Unique Kaspersky Endpoint Agent identifier.
- Unique identifiers of certificates.
- Basic part of the web address of the server with the Central Node component installed.

3. In the reports on task execution results:

- Information about the objects detected during IOC scan.
- Flags of the additional actions performed by Kaspersky Endpoint Agent upon completion of tasks (for example, "deleteFileAfterReboot": false).
- Task execution errors and return codes.
- Statuses with which the tasks were completed.
- Task completion time.
- Version of the settings used for execution of the tasks.
- Information about the objects submitted to the server, quarantined objects, and objects restored from the quarantine: paths to objects, MD5 and SHA256 hashes, identifiers of quarantined objects.
- Information about the processes started or stopped on the device with Kaspersky Endpoint Agent installed upon the server request: PID and UniquePID, error code.
- Files requested by the server.
- Telemetry packets.

- Data on running processes:
  - Name of the executable file, including the full path and extension.
  - Process autorun settings.
  - Process ID.
  - Logon session code.
  - Logon session name.
  - Date and time when the process started.
- Data on files:
  - Path to the file.
  - File name.
  - File size.
  - File attributes.
  - Date and time of file creation.
  - Date and time of the last modification of the file.
- Data indicated in errors receiving information about objects:
  - Full name of the object whose processing resulted in the error.
  - Error code.

4. Telemetry data:
   - Type of data in the registry prior to the registered modification operation.
   - Data in the registry key prior to the registered modification operation.
   - Text of the processed script or part of it.
   - Type of processed object.
   - Method of sending the command to the command shell.

Data from the requests of the Central Node component to Kaspersky Endpoint Agent:

1. Task settings:
   - Task types.
   - Task schedule settings.
   - Names and passwords of the accounts under which the tasks can be run.

- Versions of settings.
- Identifiers of quarantined objects.
- Paths to the objects.
- MD5 and SHA256 hashes of the objects.
- Command line to start the process together with the arguments.
- Flags of the additional actions performed by Kaspersky Endpoint Agent upon completion of the task.
- IOC file identifiers to be retrieved from the server.
- IOC files.
- Folders for which you want to get the results of the "Get a list of files, processes" task.
- Masks of object names and extensions for the "Get a list of files, processes" task.

2. Network isolation settings:

- Types of settings.
- Versions of settings.
- Lists of network isolation exclusions and exclusion settings: traffic direction, IP addresses, ports, protocols, and full paths to executable files.
- Flags of additional actions performed by Kaspersky Endpoint Agent.
- Time of automatic isolation disabling.

3. Settings for preventing execution and opening of documents:

- Types of settings.
- Versions of settings.
- Lists of prevention rules and rule settings: paths to objects, types of objects, MD5 and SHA256 hashes of objects.
- Flags of additional actions performed by Kaspersky Endpoint Agent.

4. Event filtering settings:

- Module names.
- Paths to objects.
- MD5 and SHA256 hashes of the objects.
- Identifiers of the entries in Windows event log.
- Digital certificate settings.

- Traffic direction, IP addresses, ports, protocols, full paths to executable files.
- User names.
- User logon types.
- Types of telemetry events for which filters are applied.

# Service data of Kaspersky Endpoint Agent

Service data of Kaspersky Endpoint Agent include:

- Data that is stored in configuration files as a result of configuring the settings by an administrator.
- Data processed as part of automatic Threat Response.
- Data processed during integration with Kaspersky Sandbox.
- Data processed during integration with the Central Node component.

Service data are stored in the %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<product version> file. Data in the Settings subfolder are encrypted using the Encrypting File System (EFS). The data is stored until Kaspersky Endpoint Agent is uninstalled.

The data can be sent to Kaspersky Security Center automatically, but is not sent to Kaspersky Sandbox.

By default, only users with System and Administrator permissions have access to the files (full access for System, read and execute for Administrator). The %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<product version> folder and the Restored subfolder are also accessible to users with User (read only) permissions.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

Kaspersky Endpoint Agent stores the following data that are processed during automatic response and integration with Kaspersky Sandbox:

1. Processed files and data entered by the user during configuration of Kaspersky Endpoint Agent settings:
   - Kaspersky Endpoint Agent access password.
   - Quarantined files.
   - Kaspersky Endpoint Agent settings.
   - Credentials of operating system users for starting tasks with certain user permissions.
   - Authentication credentials for Kaspersky Security Center Administration Server.
   - Authorization credentials for the proxy server.

- Addresses of custom update sources.
- Public key of the certificate used for integration with Kaspersky Sandbox.

2. Kaspersky Endpoint Agent cache:

- Time when scan results were written to the cache.
- MD5 hash of the scan task.
- Scan task identifier.
- Object scan result.

3. Queue of the object scan requests:

- ID of the object in the queue.
- Time when the object was queued.
- Processing status of the queued object.
- ID of the user session in the operating system where the object scan task was created.
- System identifier (SID) of the operating system user whose user account permissions were used to create the object scan task.
- MD5 hash of the object scan task.

4. Information about the tasks for which Kaspersky Endpoint Agent awaits scan results from Kaspersky Sandbox:

- Time when the object scan task was received.
- Object processing status.
- ID of the user session in the operating system where the object scan task was created.
- ID of the object scan task.
- MD5 hash of the object scan task.
- System identifier (SID) of the operating system user whose user account was used to create the task.
- XML schema of the automatically created IOC.
- MD5 or SHA256 hash of the scanned object.
- Processing errors.
- Names of the objects that the scanning task was created for.
- Object scan result.

When integrated with the Central Node component, Kaspersky Endpoint Agent stores the following data locally:

1. Processed files and data entered by the user during configuration of Kaspersky Endpoint Agent settings:
    - Quarantined files.
    - Kaspersky Endpoint Agent settings:
        - Kaspersky Endpoint Agent access password.
        - Credentials of operating system users for starting tasks with certain user permissions.
        - Authentication credentials for Kaspersky Security Center Administration Server.
        - Authorization credentials for the proxy server.
        - Addresses of custom update sources.
        - Public key of the certificate used for integration with KATA Central Node.
        - Public key of the certificate used for integration with Kaspersky Sandbox.
        - License data.
2. Data required for integration with the Central Node component:
    - Updatable telemetry filtering schemes.
    - Telemetry event packet queue.
    - Cache of IOC file identifiers received from the Central Node component.
    - Objects to be passed to the server within the Get file task.
    - Reports about the results of the "Get a list of files, processes" task.

# Data contained in Kaspersky Endpoint Agent trace files and dumps

Kaspersky Endpoint Agent can record debug information in trace files in accordance with settings to support the operation of the program.

Kaspersky Endpoint Agent dump files are created by the operating system when the program fails and are rewritten after each failure.

Trace files and dump files can include any personal data of the user or confidential data of your organization.

Do not use Kaspersky Endpoint Agent on hosts from which data transfer is forbidden by your corporate policy.

By default, Kaspersky Endpoint Agent does not record any debug information.

Trace files and dump files are never automatically sent beyond 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 and dump files are stored indefinitely and are not deleted when Kaspersky Endpoint Agent is uninstalled.

Debug information can be necessary for contacting the Technical Support.

There are no special mechanisms to limit access to trace and dump files. The administrator can take steps to configure writing this information into a secured folder.

The path for trace files and dump files is not configured by default. The administrator must manually specify a folder for writing trace files and dump files.

Data in trace files and dump files can contain the following information:

- Actions performed by Kaspersky Endpoint Agent on the host.
- Information about objects processed by Kaspersky Endpoint Agent.
- Errors occurring during the operation of Kaspersky Endpoint Agent.
- 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 Kaspersky Endpoint Agent.
- 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 Kaspersky Endpoint Agent.
- Fully qualified domain name of the computer.
- Serial number of the logical drive.
- HTTP protocol headers.
- Full paths to files on computers with Kaspersky Endpoint Agent.

- Names of files on computers with Kaspersky Endpoint Agent.
- Full names of folders on computers with Kaspersky Endpoint Agent.
- 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 sent to Kaspersky if KSN and KMP Statements are accepted

If you agree with the terms and conditions of the Kaspersky Security Network (KSN) Statement, the program automatically sends information about this to Kaspersky.

Data on acceptance of the terms and conditions of this Statement can be stored locally in the %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<version>\Data\ folder.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

The following data is sent to Kaspersky when you accept or decline the terms and conditions of the KSN Statement:

- Statement identifier (KSN, EULA).
- Statement version.
- Statement acceptance flag (1 – Statement accepted, 0 – Statement declined).
- Date when the Statement was accepted or declined.

Kaspersky can use this data to generate statistical information.

# Data in alerts and events

Event data is saved in binary form in the folder C:\ProgramData\Kaspersky Lab\Endpoint Agent\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. Kaspersky Endpoint Agent component does not manage access permissions to this folder and any files in it. It is the system administrator who determines access permissions.

Event data can contain information related to the following:

- Data on executable modules.
- Data on network connections.
- About the operating system that is installed on the computer with Kaspersky Endpoint Agent.
- 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 Kaspersky Endpoint Agent.
- 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 Kaspersky Endpoint Agent. The task completion reports are saved in archived non-encrypted form in the folder C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\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. Kaspersky Endpoint Agent component does not manage access permissions to this folder and any files in it. 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 Kaspersky Endpoint Agent.
- Files of the computer with Kaspersky Endpoint Agent.
- Names of alternate streams of NTFS
- Full paths to files on the computer with Kaspersky Endpoint Agent.
- Full names of folders on the computer with Kaspersky Endpoint Agent.
- Content of the process standard output.
- Content of the process standard error stream.

# Data contained in an install log

The administrator can enable the Kaspersky Endpoint Agent installation log (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 Agent\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. Kaspersky Endpoint Agent component does not manage access permissions to this folder and any files in it. 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:

- C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp for Kaspersky Endpoint Agent that is installed as part of Kaspersky Endpoint Security.
- C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp for Kaspersky Endpoint Agent that is installed from the Kaspersky Anti Targeted Attack Platform distribution kit.

When performing a program run task on a host, Kaspersky Endpoint Agent locally stores the contents of standard output streams and errors of the running process in plain unencrypted form until the task completion report is sent to the Central Node component. Files are stored in one of the following folders:

- C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\kata\temp for Kaspersky Endpoint Agent that is installed as part of Kaspersky Endpoint Security.
- C:\ProgramData\Kaspersky Lab\Endpoint Agent\protected\data\kata\temp for Kaspersky Endpoint Agent that is installed from the Kaspersky Anti Targeted Attack Platform distribution kit.

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. Kaspersky Endpoint Agent component does not manage access permissions to this folder and any files in it. It is the system administrator who determines access permissions.

# Program licensing

This section covers the main aspects of Kaspersky Anti Targeted Attack Platform 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 **Program 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. 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.

*To add a key to the program,*

download a key file.

Kaspersky can block a key over violations of the End User License Agreement. If the key has been blocked, 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 application depends on the type of the added license key:

- **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**, **User rules**, **Storage**, and **Endpoint Agents** have limited functionality.

# About the key file

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

1. Sign in to the Sandbox web interface using the account credentials that you specified during installation of the Sandbox component.
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 a computer with Kaspersky Endpoint Agent

On each computer with a standalone Kaspersky Endpoint Agent program 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 Kaspersky Endpoint Agent program is installed.

# Adding a key

In distributed solution 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 **Program 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.
   This opens the file selection window.
4. Select a key file to download and click the **Open** button.
   This closes the file selection window.

The key is added to the program.

# Replacing a key

In distributed solution 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 **Program 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.
   This opens the file selection window.
4. Select a key file you want to use to replace the active key and click the **Open** button.
   This closes the file selection window.

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

# Removing a key

In distributed solution 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 **Program settings** section, **License** subsection.
2. Select the type of key: **KATA** or **KEDR**.
3. In the section with the selected key type, click **Delete**.
   This opens the key removal confirmation window.

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**, **User rules**, **Storage**, and **Endpoint Agents** 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 application also depends on the type of the added license key.

- **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**, **User rules**, **Storage**, and **Endpoint Agents** have limited functionality.

# 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.
- *Kaspersky Endpoint Agent*. Installed on workstations and servers in the IT infrastructure of the organization. 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'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 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, which is a server or virtual machine on which the Kaspersky 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.

The Sensor component can be used as a proxy server for outgoing connections from the Endpoint Agent component.

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*). Analyzes and monitors network activity of software installed on computers of the corporate LAN using TAA (IOA) rules. 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.

# Kaspersky Endpoint Agent component

Kaspersky Endpoint Agent is a software component that is installed on workstations and servers in the IT infrastructure of the organization (hereinafter also referred to as "corporate LAN computers" or "computers"). On these computers, the Kaspersky Endpoint Agent continuously monitors processes, open network connections, and files that are being modified, and sends this monitoring data to the server with the Central Node component.

Computers intended for installation of Kaspersky Endpoint Agent must meet hardware and software requirements.

# Operation of the program

Kaspersky Anti Targeted Attack Platform includes two functional blocks:

- Kaspersky Anti Targeted Attack (hereinafter also referred to as "KATA"), which detects threats on the perimeter of 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.

You can use the full functionality of the program (KATA and KEDR key) or partial functionality (only KATA key or only KEDR key).

## Principle of operation of Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack includes the following components:

- Sensor.
- Central Node.
- Sandbox.

The components interact as follows:

- The Sensor component receives mirrored SPAN, ERSPAN, RSPAN traffic, objects metadata of HTTP, FTP, SMTP, and DNS protocols, HTTP and FTP traffic data, as well as HTTPS traffic (if the administrator has configured SSL certificate replacement on the proxy server), copies of email messages, and does the following with the gathered data:
  - Scans Internet traffic for signs of intrusion into the corporate IT infrastructure using the Intrusion Detection System technology (hereinafter also referred to as IDS).
  - Checks the reputation of files and URLs against the Kaspersky Security Network database (hereinafter also referred to as KSN) or Kaspersky Private Security Network (hereinafter also referred to as KPSN).
  - Sends objects and files to be scanned by the Central Node component.

  A Sensor component can also be a *mail sensor*, which is a server or virtual machine on which the Kaspersky application Kaspersky Secure Mail Gateway (KSMG) or Kaspersky Security for Linux Mail Server (KLMS) is installed.

- The Central Node component scans files and objects using anti-virus databases, YARA rule databases created by Kaspersky Anti Targeted Attack users, and if necessary, sends files and objects to be scanned by the Sandbox component.

- The Sandbox component analyzes the behavior of objects in virtual operating systems to detect malicious activity and signs of targeted attacks on corporate IT infrastructure, and sends scan results to the Central Node server.

If any threats are detected, the Central Node server records relevant information in the alert database. You can view the alert table in the **Alerts** section of the program web interface or by generating an alert report.

Alert information can also be published to a SIEM system that is used in your organization, as well as external systems. Information on Sandbox component alerts can be published in the local reputation database of Kaspersky Private Security Network.

## Principle of operation of Kaspersky Endpoint Detection and Response

Kaspersky Endpoint Detection and Response includes the following components:

- Central Node.

- Kaspersky Endpoint Agent.

  The Sensor component can be used as a proxy server for outgoing connections from Kaspersky Endpoint Agent.

The components interact as follows:

- Kaspersky Endpoint Agent is installed on individual Windows computers within the corporate IT infrastructure and continuously monitors processes, open network connections, and files being modified. Information about events on the computer is sent to the Central Node server.

  Kaspersky Endpoint Agent sends information about the following events to the Central Node server:

  - **Process started**
  - **Module loaded**
  - **Remote connection**
  - **Prevention rule**
  - **Document blocked**
  - **File created**
  - **Windows Log event**
  - **Registry modified**
  - **Port listened**

- **Driver loaded**
- **Interpreted file run**
- **Console interactive input**

Kaspersky Endpoint Agent can also integrate with Endpoint Protection Platform (hereinafter also referred to as "EPP") workstation protection programs: Kaspersky Endpoint Security and Kaspersky Security for Windows Server installed on the same computer as Kaspersky Endpoint Agent. In this case, Kaspersky Endpoint Agent also sends information about threats detected by the EPP programs and results of threat processing by these programs to the Central Node server.

The components interact as follows:

- Kaspersky Endpoint Security and Kaspersky Security for Windows Server send information about detected threats and threat processing results to Kaspersky Endpoint Agent.
- Kaspersky Endpoint Agent sends data gathered while monitoring processes, open network connections, and files being modified, as well as data received from EPP programs, to the Central Node server.

  The Central Node server processes received data and displays the corresponding events in the program web interface.

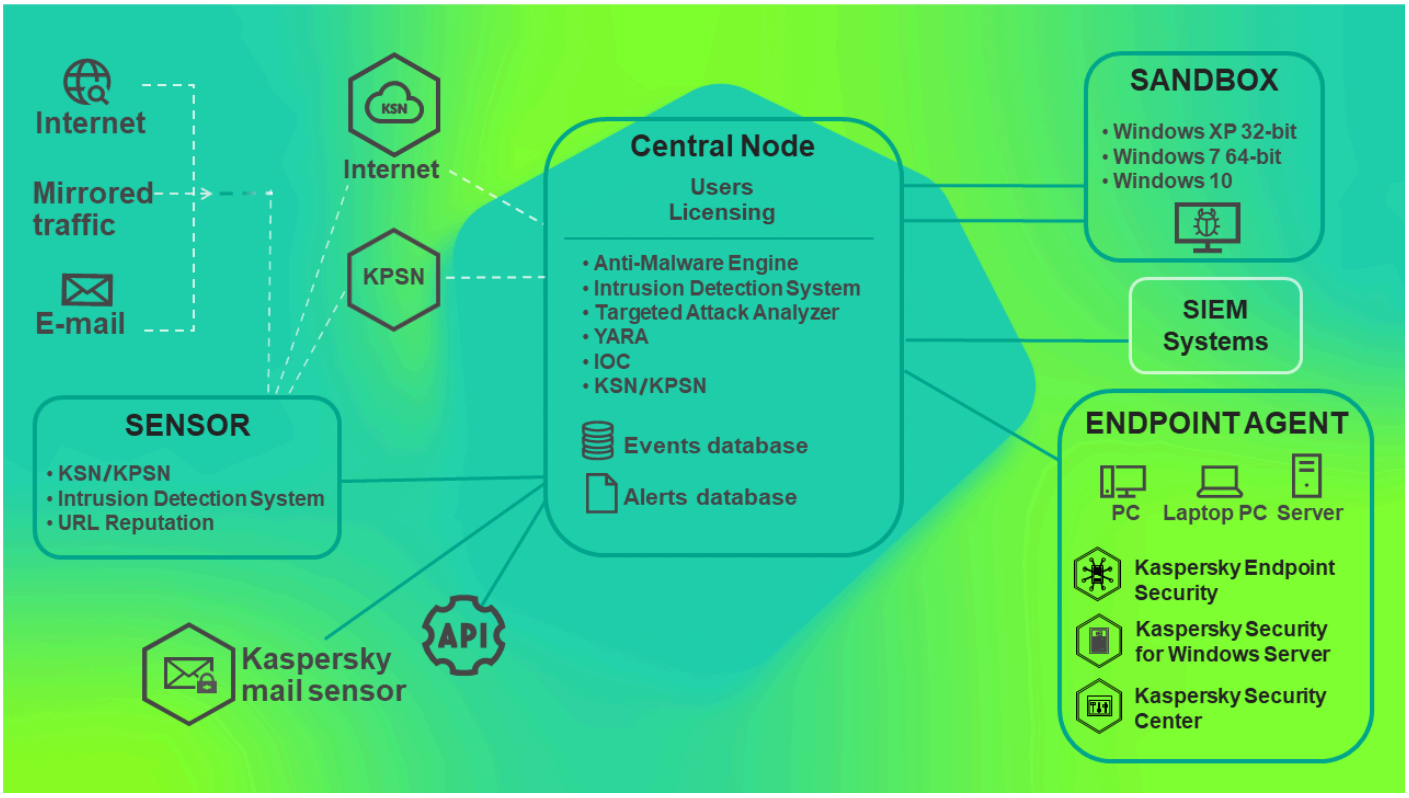
  As a result of data processing by EPP programs, **Detect** and **Detect processing result** events are generated.

  Events arriving at the Central Node server are marked by TAA (IOA) rules. As a result of this markup, alerts are generated for events that require user attention.

When the Central Node server is integrated with Kaspersky Endpoint Agent, you can do the following to react to detected threats:

- Manage files and programs by running tasks on Kaspersky Endpoint Agent hosts.
- Configure policies for preventing the running of files and processes on selected Kaspersky Endpoint Agent hosts.
- Isolate separate hosts with Kaspersky Endpoint Agent from the network.
- Work with TAA (IOA) rules to classify and analyze events.
- Work with OpenIOC compliant files (IOC files) to search for signs of targeted attacks, infected and probably infected objects on hosts with Kaspersky Endpoint Agent and in the alert database.

The principle of operation of Kaspersky Anti Targeted Attack Platform is shown in the following picture.

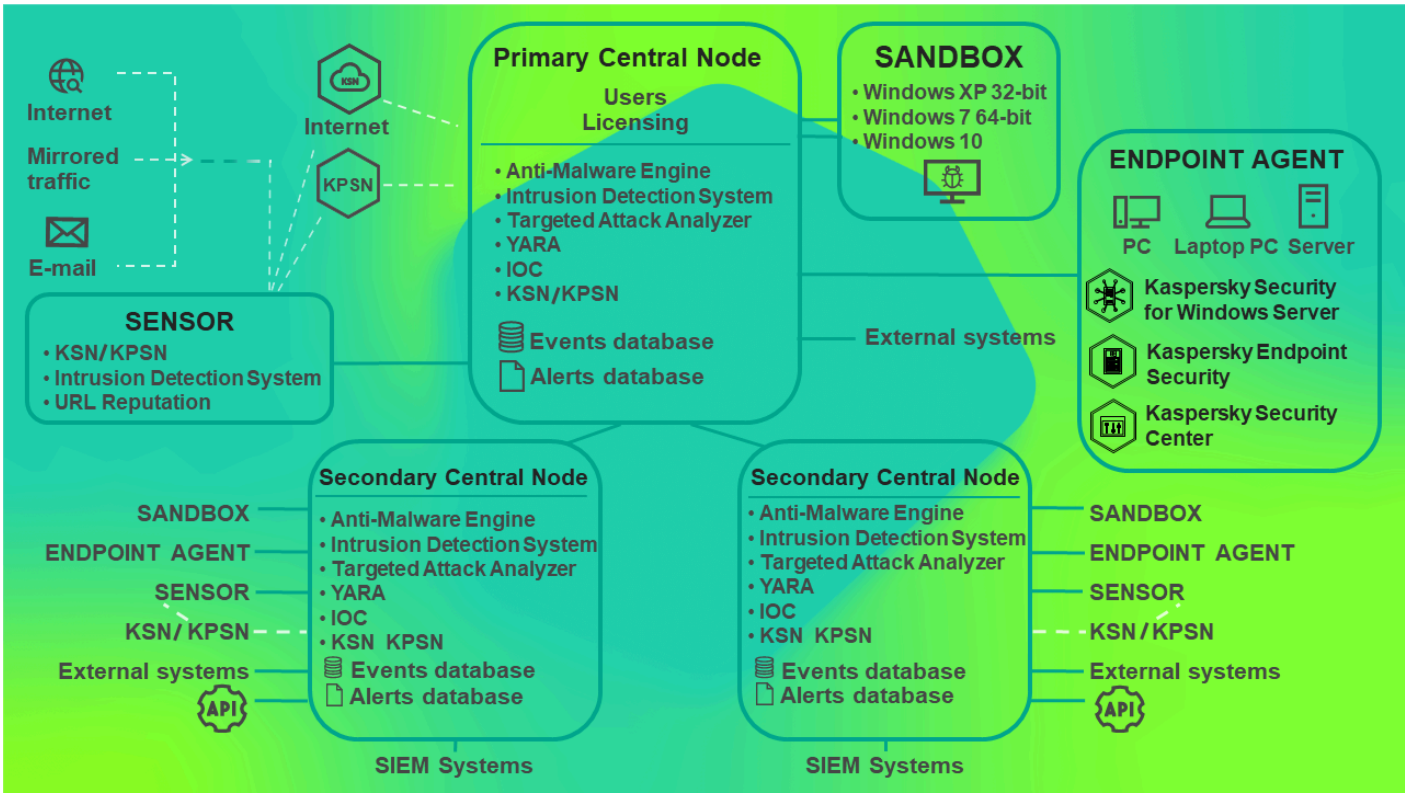



Principle of operation of Kaspersky Anti Targeted Attack Platform

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

A distributed solution 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 Kaspersky Anti Targeted Attack Platform in distributed solution mode is shown in the following picture.




Principle of operation of Kaspersky Anti Targeted Attack Platform 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.

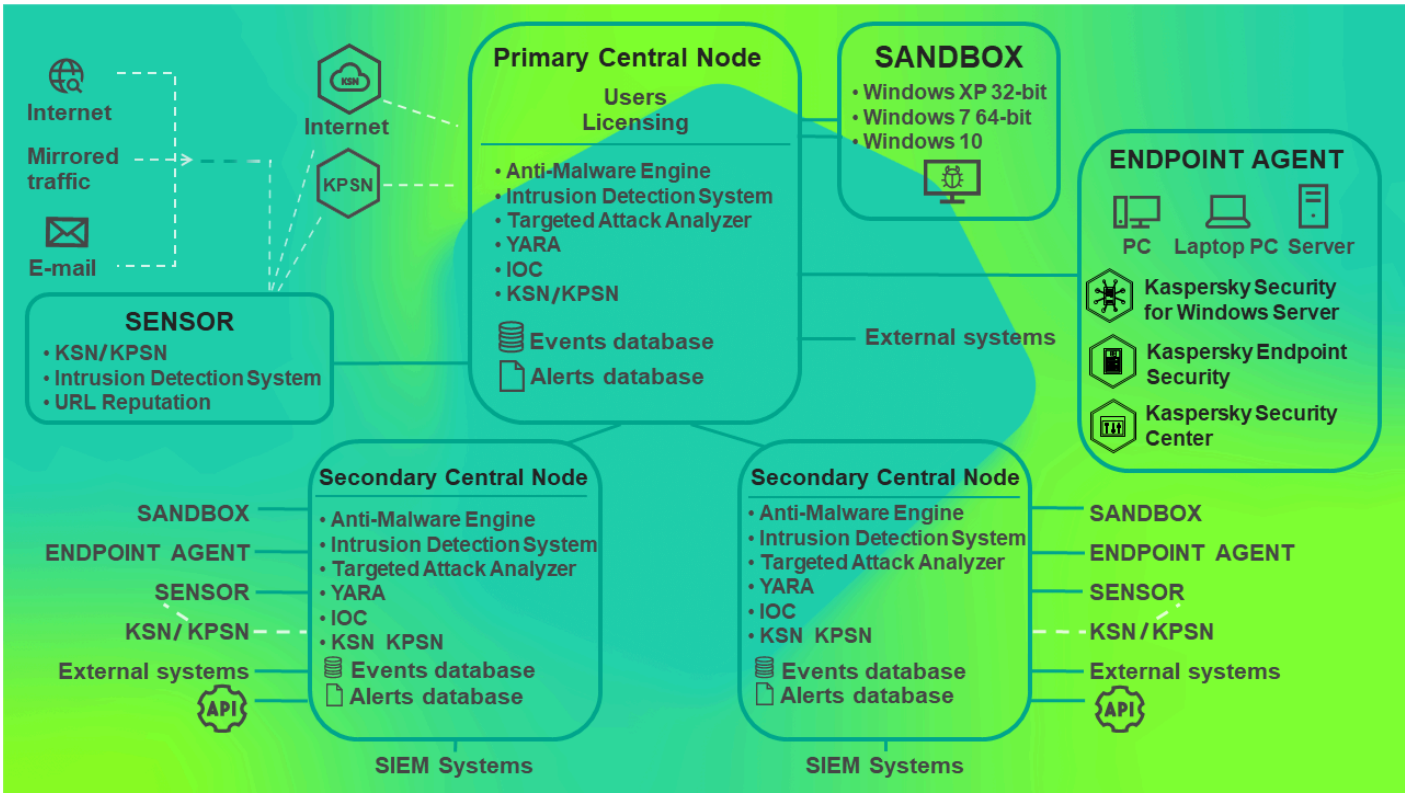
The distributed solution allows centralized management of the following functional areas of the program:

- Users.
- Alerts.
- Threat Hunting.
- Tasks.
- Prevention.
- User rules.
- Storage.
- Endpoint Agents, 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.

For each user account, the number of simultaneous program management sessions is limited to one IP address. If the same user name is used to sign in to the program from a different IP address, the earlier session is terminated.

If you are using the distributed solution and multitenancy mode, the limit is enforced for each PCN and SCN server separately.




Operation of the program in distributed solution mode

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 upgrade the Central Node component to version 3.7.

  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:

1. Installing the Central Node components.
2. Assigning the PCN role to one of the servers.
3. Assigning the SCN role to the rest of the servers and sending requests to connect to the PCN.
4. Processing a SCN to PCN connection request.

# 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.

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. | All users are deleted except the user that was created while Central Node was deployed.<br>After that, the SCN requests a list of users from the PCN and uses that list to create local users with the same parameters:<br>• Name<br>• Password<br>• Role<br>• Status<br>Users that do not have rights to access the SCN, are not displayed in the list of users. |
| 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 | On the **Alerts** tab, you can now select the SCNs whose information should be displayed in the widget.<br>On the **System health** tab, the status of connection of the PCN with connected SCNs is now displayed. | On the **System health** tab, the status of connection with the PCN is now displayed. |
| Tasks | 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.<br>Tasks created on SCNs are also displayed in the task list. Settings of these tasks cannot be changed on the PCN. | Tasks created on the PCN are displayed, as well as tasks created on this SCN.<br>Settings of tasks created on the PCN cannot be changed. |
| Reports | Templates and reports created before the switch to distributed solution mode are preserved.<br>A **Servers** column is added to the report table, containing information about the relevant SCN for the alert.<br>After switching to distributed solution mode, only reports created on an PCN are displayed. | Templates and reports created before the switch to distributed solution mode are preserved.<br>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.<br>After switching to distributed solution mode, only reports created on an SCN are displayed. |

| Functional area | PCN | SCN |
|---|---|---|
| Prevention | 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.<br>Policies created on SCNs are also displayed in the policy list. Settings of these policies cannot be changed on the PCN.<br>Presets for automatic creation of prevention rules become unavailable, new rules are not created. Rules that were previously automatically created are applied to all connected SCNs. | Policies created on the PCN are displayed, as well as policies created on this SCN.<br>Settings of policies created on the PCN cannot be changed.<br>Presets for automatic creation of prevention rules become unavailable, new rules are not created. Rules that were previously automatically created are applied only to this SCN. |
| Storage | All files and metadata that were stored on PCNs before the switch to distributed solution mode are preserved. The name of the PCN is displayed for them in the **Central Node** column.<br>The PCN also keeps the contents of the Storage of all connected SCNs. | All files and metadata that were stored on SCNs before the switch to distributed solution mode are preserved. |
| TAA exceptions | 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 | During threat hunting in the database, the PCN sends a request to all connected SCNs. After the search query is processed, a list of PCN and SCN events of the selected organization is displayed. | No changes. |
| User rules - TAA | IOC files added on the Central Node server before it was assigned the PCN role are applied to the PCN.<br>TAA (IOA) rules that were added on the Central Node server before it was assigned the PCN role are applied to the PCN. | IOC files and TAA (IOA) rules added on the PCN, as well as IOC files and TAA (IOA) rules added on this SCN before and after switching to distributed solution mode are displayed. |
| Backup of the program | Backup of the program is only available on a PCN that does not have SCNs connected.<br>To back up the program on a PCN, disconnect all SCNs from the PCN. | Backup of the program on an SCN is not available.<br>To back up the program on an SCN, disconnect that server from the PCN by switching it to standalone server mode. |
| Integration with MDR | Integration settings configured on the Central Node before it is assigned the PCN role are kept after switching to distributed solution mode and are applied to all connected SCNs. | Integration settings configured on the Central Node before it is assigned the SCN role are replaced with settings received from the PCN server after switching to distributed solution mode. |

# 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 **Cluster management** section.

3. Click **Distributed solution**.
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 **Assign the PCN role**.

   This opens the action confirmation window.

   > 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 **Cluster management** 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).
  - **State** – 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.

# 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 **Cluster management** section in the window of the program web interface.
3. Click **Distributed solution**.

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 **Cluster management** section.

8. If certificate fingerprints on the SCN and the PCN match, click **Send connection request**.

   This opens the action confirmation window.

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 **Cluster management** 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 **Certificate fingerprint from request** field of the **Cluster management** 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**.

        This opens the **Accept connection request** window.

     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.

     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 **Cluster management** 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.
  - **State** – 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.
  - **State** – 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 **Cluster management** 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 **Cluster management** section in the window of the program web interface.

3. In the **Companies** workspace, select the organization that you want to delete.

4. Click **Delete**.

   This opens the action confirmation window.

   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 **Cluster management** 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 **Save**.

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 **Cluster management** 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**.

   This opens the action confirmation window.

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 **Cluster management** section in the window of the program web interface.

3. Click **Disconnect**.

   This opens the action confirmation window.

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.

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.<br>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.<br>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.<br>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.<br>Information about users who created policies on the SCN is preserved.<br>Presets for automatically creating prevention rules become available. By default, presets are disabled after disconnecting the SCN from the PCN. |
| Storage | All objects related to the disconnected SCN are deleted from Storage. | All objects in the Storage are preserved.<br>The link to the task stops working in information about objects received as part of tasks created on the PCN. |
| TAA exceptions | No changes. | No changes. |

| Functional area | PCN | SCN |
|---|---|---|
| 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. |
| User rules - TAA and IOC | IOC and TAA (IOA) rules of a disconnected SCN are deleted. | IOC and TAA (IOA) rules created on the PCN are deleted. |
| Backup of the program | Backup of the program remains unavailable. | Backup of the program becomes available. |
| Integration with MDR | No changes. | Integration settings are kept.<br>After disconnecting the SCN from the PCN, you can modify settings on the SCN side. After disconnecting the SCN from the PCN, you still cannot modify settings on the PCN side. |

# 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:

1. **Deleting all data on the SCN**
2. Disconnecting the SCN from the PCN through the PCN web interface
3. Disconnecting the SCN from the PCN through the SCN web interface
4. **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 **Cluster management** section in the window of the program web interface.

3. In the server list, select the SCN that you want to delete.

4. Click **Delete**.

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.

# Sizing Guide

To obtain and maintain optimum performance under varying operational conditions of the program, you must take into account the number of networked devices, network topology, and the set of program features that you need.

Selection of the optimal program configuration consists of the following steps:

1. Selecting a common deployment scenario
2. Calculating hardware requirements using the sizing calculator

# 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.

Kaspersky Endpoint Agent can be installed on any computers that belong to the organization's IT infrastructure and run the Windows operating system. Outbound connections from computers with Kaspersky Endpoint Agent 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 mode.

The deployment scenario selection depends on the utilized program functionality. 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 5000 Kaspersky Endpoint Agent programs 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 hosts to Kaspersky Endpoint Agent and the Central Node. One Sensor component supports the connection of up to 1000 Kaspersky Endpoint Agent hosts.

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.

Selecting a deployment scenario when using KATA and KEDR functionality

| Criterion | Two-server scenario | Three-server scenario | Four- or more server scenario | Distributed solution |
|---|---|---|---|---|
| Network traffic and mail traffic cannot be received on the same device. | No | Yes | Yes | Yes |
| Number of Kaspersky Endpoint Agent hosts | No | 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. | No | One | Two or more | Two or more |
| The capacities of one Sandbox component are insufficient to analyze all objects within acceptable time frames. | No | No | 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.

Selecting a deployment scenario when using KATA functionality

| Criterion | Two-server scenario | Three-server scenario | Four- or more server scenario |
|---|---|---|---|
| Network traffic and mail traffic cannot be received on the same device. | No | 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. | No | One | Two or more |
| The capacities of one Sandbox component are insufficient to analyze all objects within acceptable time frames. | No | No | 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
- With a Sandbox component

## Two-server deployment scenario

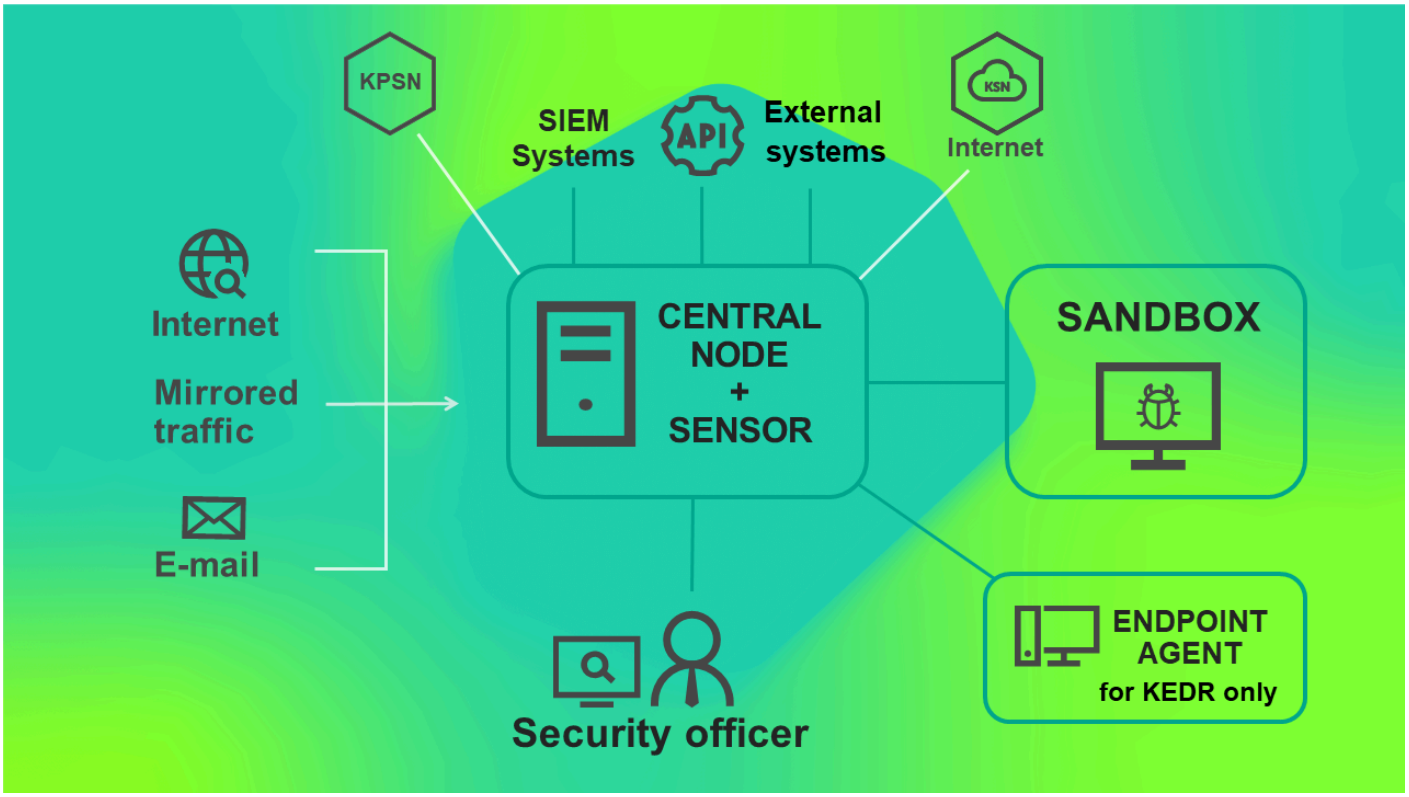
When using KATA and KEDR functionality, you can install the Kaspersky Endpoint Agent program on corporate LAN computers. When using KATA functionality, the Kaspersky Endpoint Agent program is not installed.

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.




Program operating scenario when deployed on two servers

# Three-server deployment scenario.

When using KATA and KEDR functionality, you can install the Kaspersky Endpoint Agent program on corporate LAN computers. When using KATA functionality, the Kaspersky Endpoint Agent program is not installed.

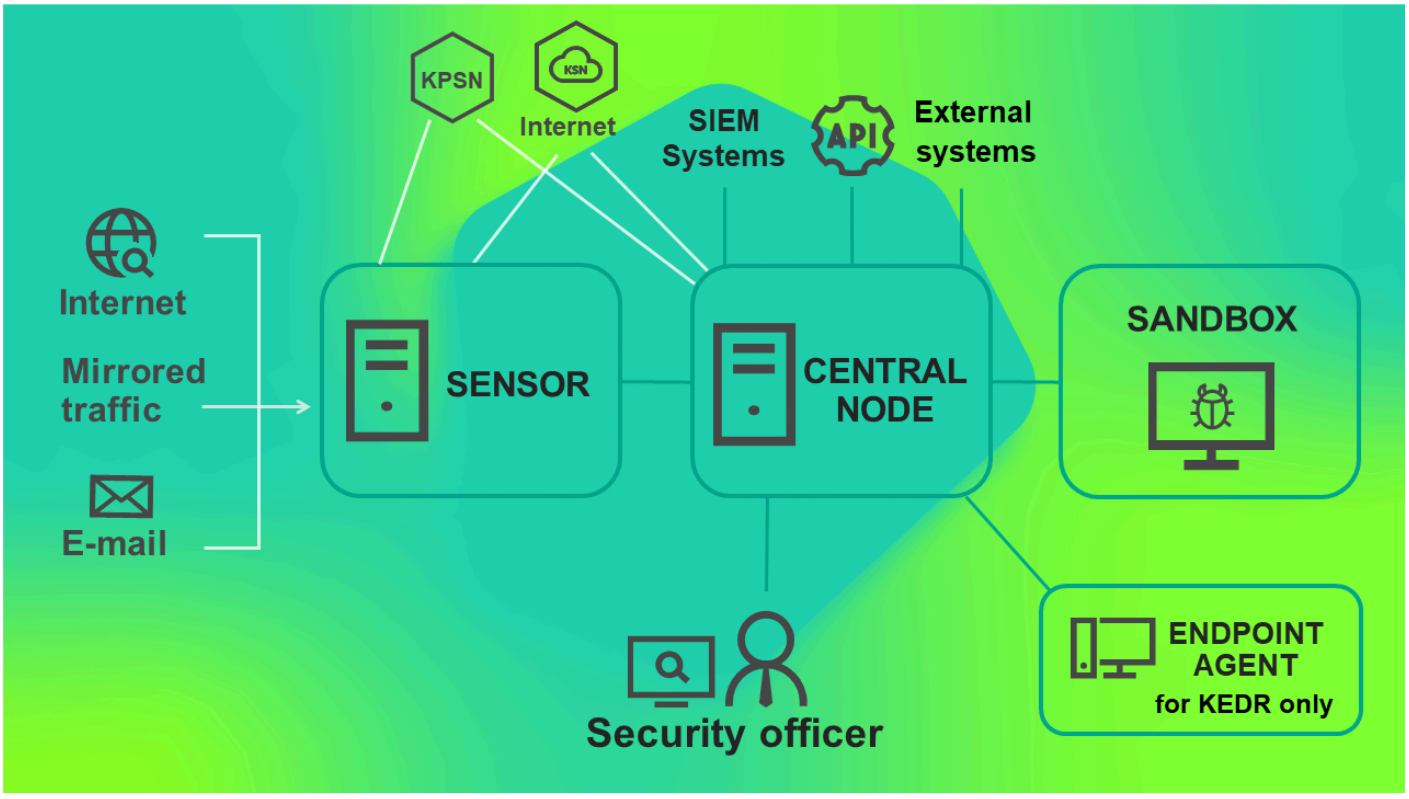
The Central Node component is always installed together with the Sensor component. If you need to use the Central Node component separately, do not configure the Sensor component.

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.




Program operating scenario when deployed on three servers

# Scenario of deployment on four or more servers.

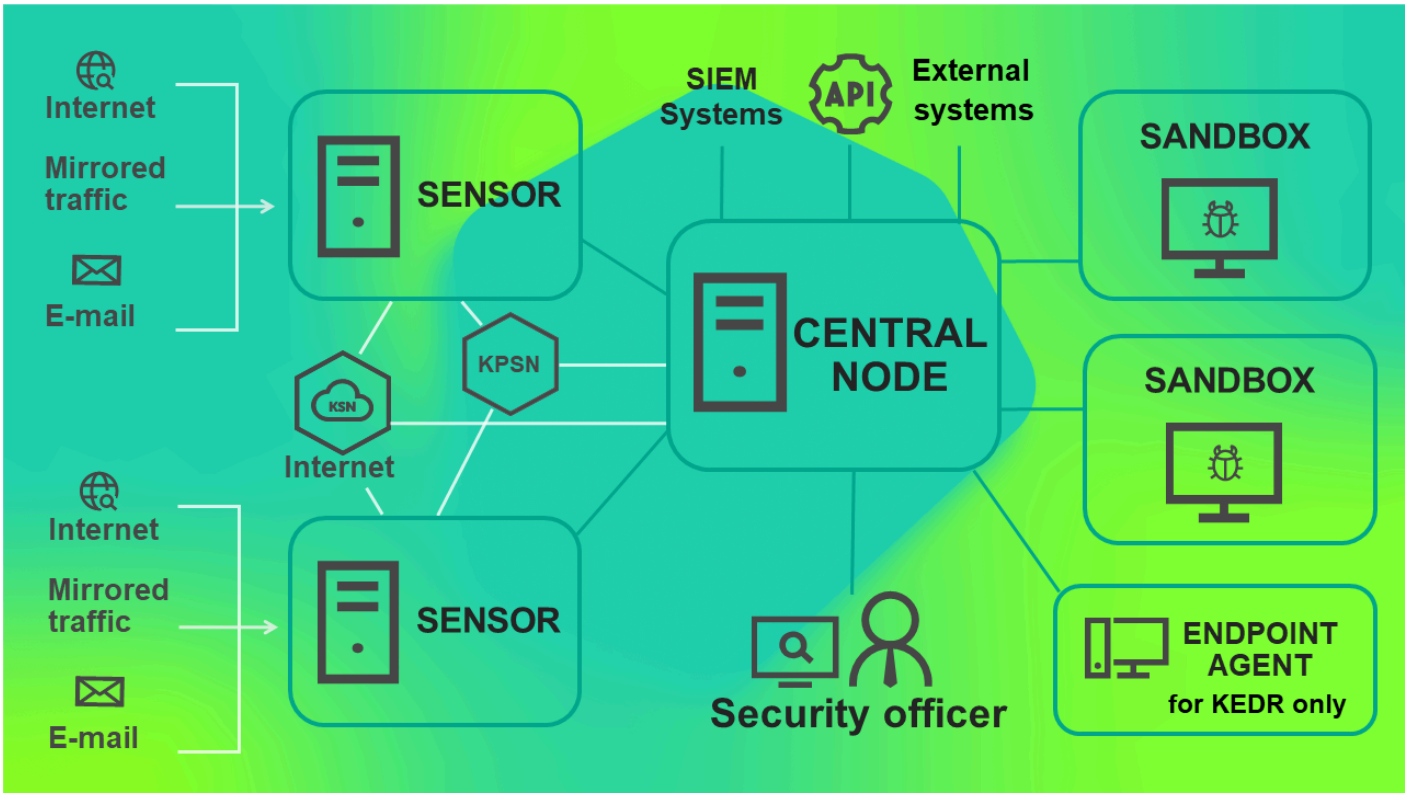
When using KATA and KEDR functionality, you can install the Kaspersky Endpoint Agent program on corporate LAN computers. When using KATA functionality, the Kaspersky Endpoint Agent program is not installed.

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 operating schematic of the program when deployed on four or more servers is presented in the figure below.

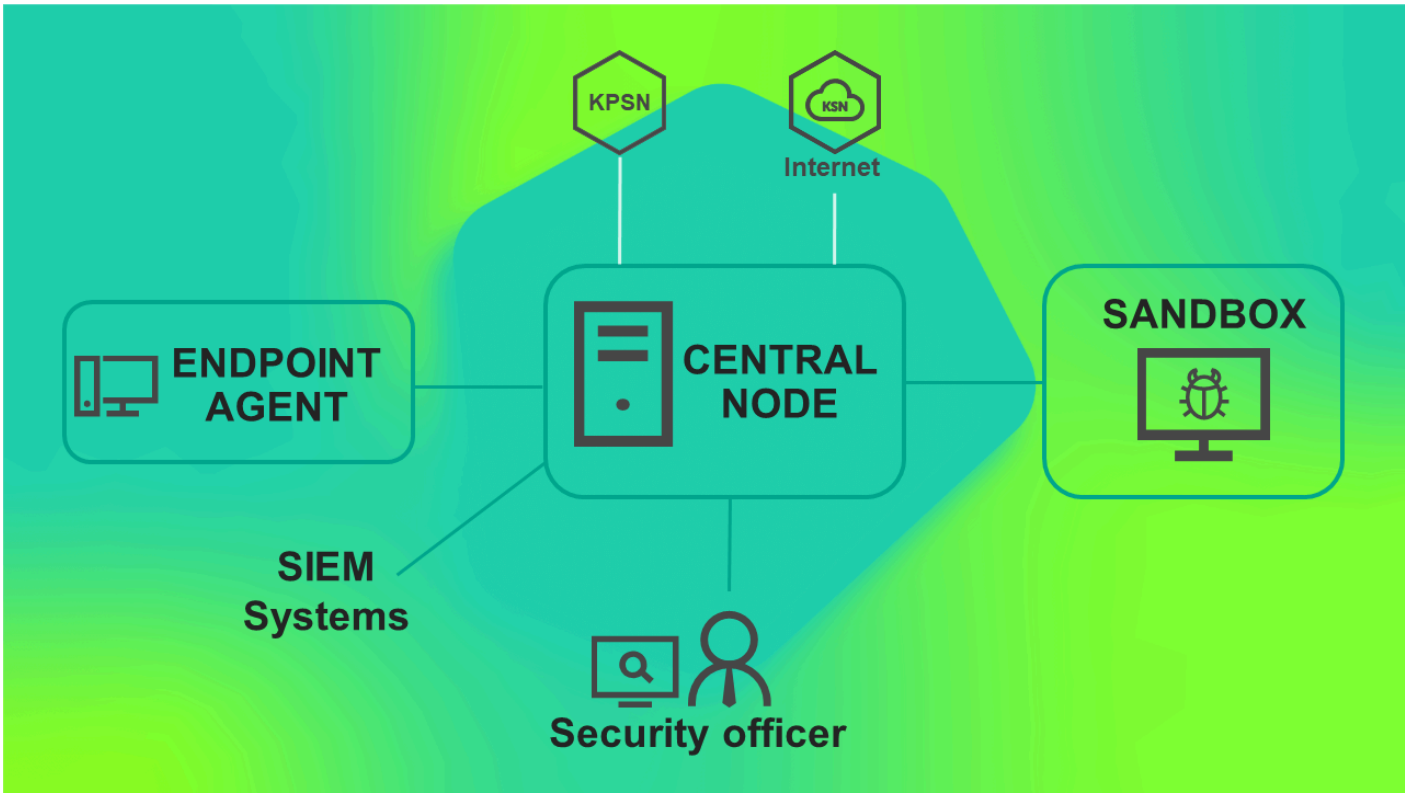



Program operating scenario when deployed on four or more servers

# 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.

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



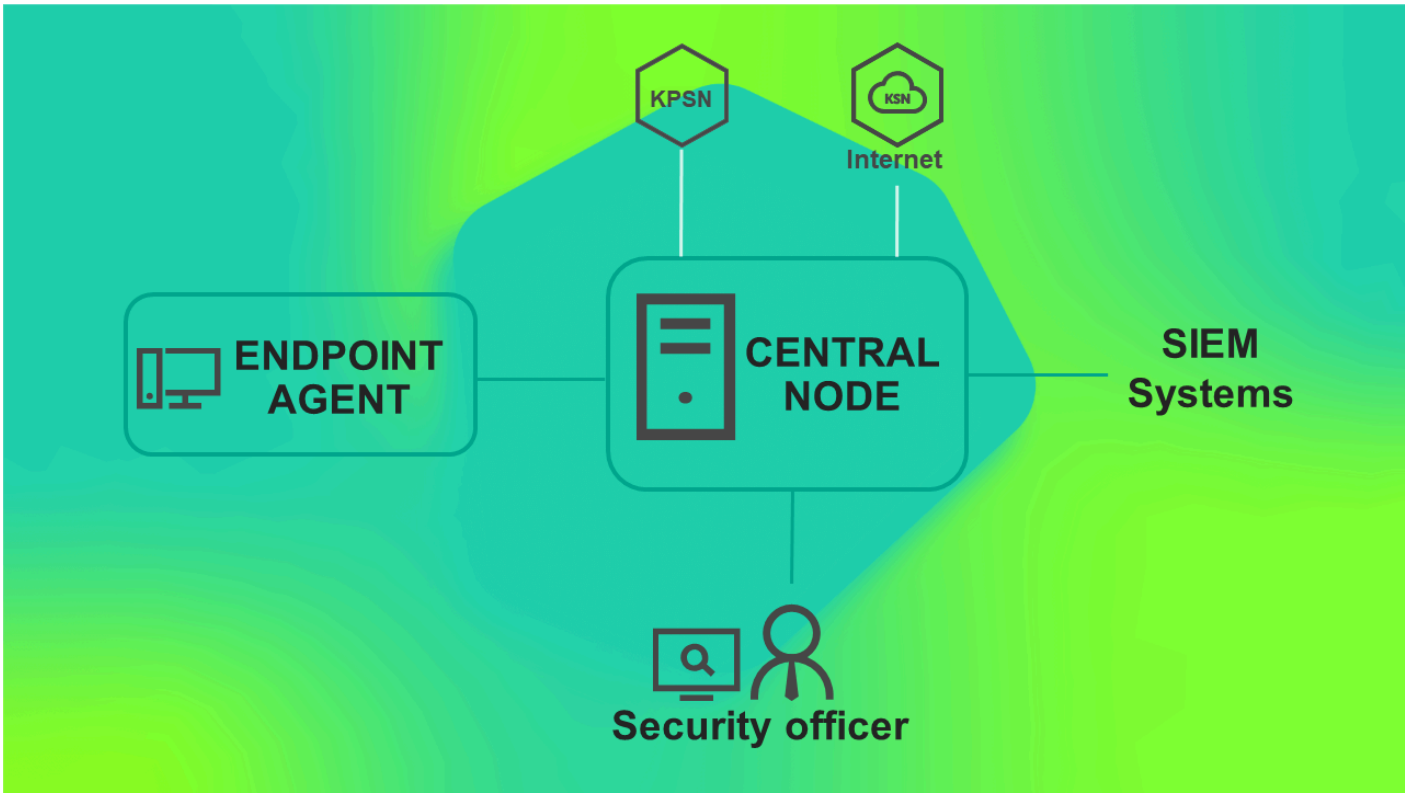

Program operating scenario when deploying KEDR functionality with the Sandbox component

## Scenario for deploying KEDR functionality without a Sandbox component

You do not need to install the Sandbox component and can use the Central Node component only for managing the Kaspersky Endpoint Agent program and data analysis.

> 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.

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




Program operating scenario when deploying KEDR functionality without the Sandbox component

# Sizing calculator

After you have selected the deployment scenario that is most appropriate for your IT infrastructure, you must calculate the hardware requirements for servers used for installing program components.

## Calculations for the Sensor component

These calculations also apply when the program is deployed on a virtual platform.

When calculating the hardware requirements for the Sensor component, you must take into account that the maximum volume of processed traffic for one Sensor component is 4 Gbps. The most resource-intensive technology is the Intrusion Detection System.

You can use a server hosting the Sensor component as a proxy server during data exchange between Kaspersky Endpoint Agent and the Central Node component to simplify configuration of network rules. For example, if Kaspersky Endpoint Agent computers are located on a separate segment of the network, it will suffice to configure a connection between servers with the Central Node and Sensor components.

When configuring the forwarding of Kaspersky Endpoint Agent traffic to the Central Node component, the following limitations apply:

- A maximum of 15,000 Kaspersky Endpoint Agent computers can connect to a single Central Node component.
- 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.

The hardware requirements for a server with the Sensor component depend on the volume of processed traffic. The required bandwidth of the communication channel between servers with the Central Node and Sensor components is the sum of the traffic of the Sensor component (10% of the traffic at the SPAN port + mail traffic + traffic over the ICAP protocol) and the requirements of the communication channel between the Central Node component and Kaspersky Endpoint Agent components (depending on the number of Kaspersky Endpoint Agent computers whose traffic the Sensor component redirects to the Central Node component).

If the bandwidth of the communication channel is more than 2 Gbps, you must **configure the use of one processor core for processing network interrupts**.

1. On the server with the Sensor component, in the file named /var/opt/kaspersky/apt-preprocessor/preprocessor.conf, add the string `pcap_cores=$CORES-1`, where `$CORES` is the number of logical cores of the server.
2. Restart the service to apply the changed parameters. To do so, run the following command:

   ```
   systemctl restart apt-preprocessor.service
   ```

3. In the file named /etc/sysconfig/irqbalance, add one of the following strings:
   - If you specified `pcap_cores=31` at the first step, add `IRQBALANCE_BANNED_CPUS=80000000`
   - If you specified `pcap_cores=47` at the first step, add `IRQBALANCE_BANNED_CPUS=8000.00000000`
4. Restart the service to apply the changed parameters. To do so, run the following command:

   ```
   service irqbalance restart
   ```

## Hardware requirements for the Sensor component depending on the processed traffic

The Sensor component can be integrated with the IT infrastructure of an organization as follows:

- Receive mirrored traffic from network devices from SPAN ports.
- Connect to a mail server over the POP3 protocol.
- Connect to a mail server over the SMTP protocol.
- Receive traffic from a proxy server over the ICAP protocol.

The hardware requirements for the Sensor component are listed in the table below. The calculations are provided for a case in which the Sensor component does not process email messages or traffic over the ICAP protocol. If the Sensor component forwards traffic from Kaspersky Endpoint Agent computers, link requirements must also be taken into account.

Hardware requirements for the Sensor component depending on the volume of processed traffic from SPAN ports

| Maximum number of Kaspersky Endpoint Agent hosts. | Maximum volume of processed traffic (Mbps) | Minimum RAM (GB) | Minimum number of logical cores |
|---|---|---|---|
| 10000 | 100 | 16 | 4 |
| 15000 | 500 | 16 | 8 |
| 15000 | 1000 | 24 | 16 |
| 15000 | 2000 | 32 | 32 |
| 15000 | 4000 | 32 | 48 |

The hardware requirements for a Sensor component that is integrated with a mail server are presented in the table below. The calculations are provided for a case in which the Sensor component does not process mirrored traffic or traffic over the ICAP protocol.

Hardware requirements for a Sensor component that is integrated with a mail server

| Maximum number of email messages per second | Minimum RAM (GB) | Minimum number of logical cores |
|---|---|---|
| 1-4 | 16 | 4 |
| 5-20 | 16 | 8 |

Processing traffic over the ICAP protocol requires less resources than processing email messages.

If the same Sensor component is used to process different protocol traffic, keep in mind the following recommendations:

- Simultaneous processing of traffic over the ICAP protocol and from SPAN ports is recommended for analysis of objects transmitted through a proxy server over the HTTPS protocol.

  To process traffic over the HTTPS protocol, the proxy server must support server certificate replacement.

- When integration with mail sensors is configured, it is not practical to extract SMTP traffic from SPAN traffic.

## Disk space requirements on a server with the Sensor component

It is recommended to use a RAID 1 disk array. The total disk space must be at least 500 GB. The minimum free disk space requirements for different data types are presented in the table below.

Minimum requirements for disk space on a server with the Sensor component

| Data type | Disk space (GB) |
|---|---|
| Redis database dump | 16 |
| Operating system | 25 |
| Temporary files | 32 |
| Trace files and update packages | 151 |
| **Total** | **224** |

If the volume of processed traffic is greater than 1 Gbps, it is recommended to allocate at least 600 GB of disk space.

# Calculations for the Central Node component

If the program is deployed to a virtual platform, CPU resource requirements are to be increased by 10 percent. In virtual disk settings, a Thick Provision disk type must be selected.

## Hardware requirements for a server with the Central Node and Sensor components

The hardware requirements for a server on which the Central Node and Sensor components are installed depend on the following conditions:

- Volume of processed traffic
- Number of email messages processed per second
- Number of Kaspersky Endpoint Agent computers.

  Kaspersky Endpoint Agent can be installed on a terminal server, file server, or network attached storage (NAS).

  If Kaspersky Endpoint Agent is installed on a terminal server, the load generated by the component is calculated as follows: one Kaspersky Endpoint Agent program on a terminal server serving X users generates the same load as X Kaspersky Endpoint Agent programs on a workstation (X users = X Kaspersky Endpoint Agent programs).

  If Kaspersky Endpoint Agent is installed on a file server or NAS, the load generated by the component is calculated as follows: one Kaspersky Endpoint Agent program on a file server or NAS generates the same load as 20 Kaspersky Endpoint Agent programs on a workstation.

If the volume of processed traffic is greater than 1 Gbps, it is recommended to install Central Node and Sensor components on separate servers.

On the server with the Central Node component, it is recommended to use two RAID disk subsystems:

- The first RAID 1 or RAID 10 disk subsystem is used for all the data specified in the table below, except for the Targeted Attack Analyzer database.
- The second RAID 10 disk subsystem is used for the Targeted Attack Analyzer database and for storing some of the logs.

The hardware requirements for the server with the Central Node component depending on the utilized functionality are presented in the table below.

Hardware requirements for the server with the Central Node component when using KEDR functionality

| Maximum number of Kaspersky Endpoint Agent computers | Minimum RAM (GB) | Minimum number of logical cores | First disk subsystem | | | | Second disk subsystem | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | ROPS (read operations per second) | WOPS (write operations per second) | RAID disk array size (TB) | The number of disks in a RAID disk array | ROPS (read operations per second) | WOPS (write operations per second) | RAID disk array size (TB) | The number of disks in a RAID disk array |
| 1000 | 64 | 8 | 100 | 1000 | 1 | 4 | 300 | 200 | Depends on the preferred storage policy | 4 |
| 3000 | 80 | 12 | 100 | 1000 | 1 | 4 | 700 | 500 | | 6 |
| 5000 | 96 | 12 | 100 | 1000 | 1 | 4 | 1000 | 600 | | 6 |
| 10000 | 160 | 20 | 100 | 1000 | 1 | 4 | 2000 | 800 | | 10 |
| 15000 | 192 | 32 | 100 | 1000 | 1 | 4 | 2000 | 800 | | 12 |

Hardware requirements for the server with the Central Node component when using KATA and KEDR functionality

| Maximum number of Kaspersky Endpoint Agent computers | Maximum number of email messages per second | Maximum volume of traffic from SPAN ports on the server with the Central Node component | Maximum volume of traffic from SPAN ports on servers with the Sensor component | Minimum RAM (GB) | Minimum number of logical cores | First disk subsystem | | | | Sec |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | ROPS (read operations per second) | WOPS (write operations per second) | RAID disk array size (TB) | The number of disks in a RAID disk array | ROPS (read operations per second) | op |
| 1000 | 1 | 200 | Not processed | 96 | 12 | 100 | 1000 | 1.9 | 4 | 300 | |
| 2000 | 2 | 500 | Not processed | 128 | 20 | 100 | 1000 | 2 | 4 | 500 | |
| 5000 | 1 | 1000 | Not processed | 160 | 36 | 100 | 1000 | 2 | 4 | 1000 | |
| 10000 | 2 | 1000 | Not processed | 192 | 40 | 100 | 1000 | 2 | 4 | 2000 | |
| 5000 | 5 | Not processed | 2000 | 144 | 20 | 100 | 1000 | 1.9 | 4 | 1000 | |
| 10000 | 20 | Not processed | 4000 | 192 | 36 | 100 | 1000 | 1.9 | 4 | 2000 | |
| 15000 | 20 | Not processed | 4000 | 256 | 48 | 100 | 1000 | 1.9 | 4 | 2000 | |

## Disk space requirements on the server with the Central Node component

When no Sensor component is used on the server with the Central Node component, it is obligatory to have at least 2000 GB of free space on the first disk subsystem and at least 2400 GB on the second disk subsystem. The amount of space required on the second disk subsystem depends on the preferred storage policy and can be calculated using the following formula:

```
150 GB + <number of Endpoint Agent components>/15000 * (400 GB + 240 GB * <number of days to store data>)
```

This formula can be used to roughly estimate the required disk space. The actual amount of stored data depends on the traffic profile of the organization and may differ from the calculated result.

The minimum free disk space requirements for each data type are presented in the table below.

Minimum requirements for disk space on the server with the Central Node component when no Sensor component is used

| Data type | First disk subsystem (GB) | Second disk subsystem (GB) |
|---|---|---|
| Targeted Attack Analyzer database | 0 | 1500 |
| Database of detected objects | 50 | 0 |
| Queues of detection technologies | 390 | 0 |
| Task queue | 1 | 0 |
| Data received after analysis by the Sandbox component | 300 | 0 |
| Quarantine | 300 | 0 |
| Files awaiting rescan | 300 | 0 |
| Redis database dump file | 16 | 0 |
| Operating system | 25 | 0 |
| Temporary files | 64 | 0 |
| Trace files | 50 | 100 |
| Update packages | 1 | 0 |
| **Total** | **1497** | **1600** |

When the Sensor component is used on the server with the Central Node component, it is obligatory to have at least 1900 GB of free space on the first disk subsystem and at least 3900 GB on the second disk subsystem. The minimum free disk space requirements for each data type are presented in the table below.

Minimum requirements for disk space on the server with the Central Node component when a Sensor component is used

| Data type | First disk subsystem on the server with the Central Node component (GB) | Second disk subsystem on the server with the Central Node component (GB) | Disk space on a server with the Sensor component (GB) |
|---|---|---|---|
| Targeted Attack Analyzer database | 0 | 1500 | 0 |
| Database of detected objects | 50 | 0 | 0 |
| Queues of detection technologies | 390 | 0 | 0 |
| Task queue | 1 | 0 | 0 |
| Data received after analysis by the Sandbox component | 300 | 0 | 0 |
| Quarantine | 300 | 0 | 0 |
| Files awaiting rescan | 300 | 0 | 0 |
| Redis database dump file | 16 | 0 | 16 |
| Operating system | 25 | 0 | 25 |
| Temporary files | 32 | 0 | 32 |
| Trace files | 50 | 100 | 150 |
| Update packages | 1 | 0 | 1 |
| **Total** | **1465** | **1600** | **224** |

If you have configured integration with the external system using REST API, you must allocate additional resources required for processing objects of this system. Additional hardware requirements are presented in the table below.

Hardware requirements for the server with the Central Node component with integrated external systems

| Number of processed objects per second | Number of additional logical cores | The number of additional servers with the Sandbox component |
|---|---|---|
| 8 | 2 | 1 |
| 16 | 4 | 2 |
| 24 | 7 | 3 |

## Requirements for the PCN server in distributed solution mode

If the load on the SCN servers is light, hardware requirements for the PCN server are the same as for a server with Central Node component in standalone mode.

Hardware requirements for the PCN server with more than 10 SCN servers under heavy load are listed in the table below.

Hardware requirements for the PCN server

| Maximum number of Kaspersky Endpoint Agent computers | Maximum number of email messages per second | Maximum volume of traffic from SPAN ports (Mbps) | Minimum RAM (GB) | Minimum number of logical cores | First disk subsystem | Second disk subsystem | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | ROPS (read operations per second) | WOPS (write operations per second) | RAID disk array size (TB) | The number of disks in a RAID disk array | ROPS (read operations per second) | WOPS (write operations per second) | RAI dis arra siz (TB |
| 10000 | 0 | 0 | 160 | 24 | 100 | 1000 | 1 | 4 | 800 | 800 | 4 |
| 1000 | 1 | 200 | 112 | 40 | 100 | 1000 | 1.9 | 4 | 600 | 600 | 1.3 |
| 5000 | 5 | 2000 | 160 | 28 | 100 | 1000 | 1.9 | 4 | 300 | 300 | 2.5 |
| 10000 | 20 | 4000 | 208 | 40 | 100 | 1000 | 1.9 | 4 | 1000 | 800 | 4 |

## Communication channel requirements

The minimum requirements for the communication channel between computers with Kaspersky Endpoint Agent and the server with the Central Node component are presented in the table below.

Minimum requirements for the communication channel between hosts with Kaspersky Endpoint Agent and the server with the Central Node component

| Maximum number of Kaspersky Endpoint Agent computers | Required bandwidth of the communication channel reserved for Kaspersky Endpoint Agent computers (Mbps) |
|---|---|
| 10 | 1 |
| 50 | 2 |

| Maximum number of Kaspersky Endpoint Agent computers | Required bandwidth of the communication channel reserved for Kaspersky Endpoint Agent computers (Mbps) |
|---|---|
| 100 | 3 |
| 1000 | 20 |
| 10000 | 200 |

Minimum requirements for the communication channel between the PCN and SCN servers in distributed solution mode are listed in the table below.

Minimum requirements for the communication channel between the PCN and SCN servers

| Maximum number of Kaspersky Endpoint Agent computers | Maximum number of email messages per second | Maximum volume of traffic from SPAN ports (Mbps) | Required communication channel bandwidth (Mbps) |
|---|---|---|---|
| 5000 | 5 | 2000 | 20 |
| 10000 | 20 | 4000 | 30 |

# Calculations for the Sandbox component

The hardware requirements for a server with the Sandbox component depend on the type and volume of processed traffic and on the permissible object scan time.

By default, the permissible object scan time is 1 hour. To reduce this time, you need a more powerful server or more servers with the Sandbox component.

It is recommended to calculate the configuration of the Sandbox component as follows:

1. Install the Central Node and Sensor components on one server and the Sandbox component on a different server for pilot operation of the program.

   To receive sufficient statistical data, the program must process traffic of the organization for a week.

2. Send the /var/log/kaspersky/apt-history/apt-history.log file, which contains the log of the program, to Kaspersky personnel for analysis.

   If multiple virtual machines are started simultaneously, the speed of processing objects from the queue is increased.

## Hardware requirements for the server hosting the Sandbox component

The calculation of the number of servers with the Sandbox component depending on the load is shown in the table below.

Hardware requirements of the Sandbox component depending on the volume of processed traffic

| Maximum number of email messages per second | Maximum volume of traffic from SPAN ports (Mbps) | Maximum number of Kaspersky Endpoint Agent computers | Number of physical servers with the Sandbox component |
|---|---|---|---|
| 1 | 200 | 1000 | 1 |
| 2 | 500 | 3000 | 1 |

| Maximum number of email messages per second | Maximum volume of traffic from SPAN ports (Mbps) | Maximum number of Kaspersky Endpoint Agent computers | Number of physical servers with the Sandbox component |
|---|---|---|---|
| 1 | 1000 | 5000 | 1 |
| 5 | 2000 | 5000 | 1 |
| 20 | 4000 | 10000 | 2 |

The estimation of the number of Sandbox components is listed for servers with the following configuration:

- When installing the Sandbox component on a physical server:
  - 2 Intel® Xeon® 8 Core™ (HT) CPUs
  - 80 GB of RAM
  - 2 HDDs, 300 GB each
- When installing the Sandbox component on a VMware ESXi virtual machine:
  - Intel Xeon 15 Core (HT) CPU, 2.1 GHz or higher;
  - 32 GB of RAM
  - 300 GB HDD

    On the virtual machine:

    1. Nested virtualization enabled.
    2. Latency Sensitivity option set to High.
    3. Entire RAM is reserved.
    4. Entire CPU frequency is reserved.

When installing the Sandbox component on a VMware ESXi virtual machine, you must set the limit for simultaneously running virtual machines to 12.

The performance of 3 or 4 virtual machines of the Sandbox component is identical to one Sandbox component on a physical server.

# Installing and performing initial configuration of the solution

This section contains instructions on installation and initial configuration of Kaspersky Anti Targeted Attack Platform.

## 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. Ensure that the servers, the computer intended for working with the program web interface, and the computers to be installed with Kaspersky Endpoint Agent all satisfy the hardware and software requirements.
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 10000 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 Kaspersky Endpoint Agent.
- 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.
- TCP 4443 when forwarding traffic from Kaspersky Endpoint Agent computers through the server with the Sensor component to the server with the Central Node component.

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 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.

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 forwarding traffic from Kaspersky Endpoint Agent computers 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 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.
- TCP 4443 when forwarding traffic from Kaspersky Endpoint Agent computers to the server with the Central Node component.

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 of Kaspersky Endpoint Agent computers 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:*

1. Start the hypervisor. For example, VMware ESXi.
2. Open the virtual machine management console.
3. 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.
4. On the **Virtual Hardware** tab, expand the **CPU** settings group and select the **Expose hardware-assisted virtualization to guest OS** check box.
5. On the **VM Options** tab in the **Latency Sensitivity** drop-down list, select **High**.
6. 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.
5. Configure the Central Node and Sensor components.

   **If there are multiple Central Node components, you can use the program in distributed solution mode.**

   **If there are multiple Sensor components, you can install and configure the Sensor component 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.**
6. **Install Kaspersky Endpoint Agent on computers in the corporate IT infrastructure.**

   You can install Kaspersky Endpoint Agent as part of EPP programs or separately.

# Installation: Sandbox component

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

*To begin the installation of the Sandbox component:*

1. Run the disk image containing the Sandbox component.

   The Setup Wizard starts.

2. Click **Ok**.

## 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** and press **ENTER**.

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

2. Please read the End User License Agreement.

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

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

4. Please carefully read the Privacy Policy.

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

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 and press **ENTER**.

   If the disk is not empty, a window is displayed asking you to confirm that you want to format the disk and install the program.

2. Click **Install**.

   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. Assigning the host name

At this step, assign a server host name to be used by DNS servers.

*To assign a server host name:*

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 4. Selecting the management 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:

- Management 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. Adding DNS server addresses

*To add DNS server addresses:*

1. In the **DNS servers** window, select **New** and press **ENTER**.
   This opens the DNS server address entry window.
2. In the **DNS server** text box, enter the IP address of the primary DNS server in IPv4 format.
3. Click **Ok**.
   The DNS server address entry window is closed.
4. If you want to add the IP address of an additional DNS server, repeat the steps in the **DNS servers** window.
5. When you are done adding DNS servers, in the **DNS servers** window, select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

## Step 7. Configuring a static network route

*To configure a static network route:*

1. In the **IPv4 Routes** window, select **New** and press **ENTER**.
   This opens the **IPv4 Static Route** window.

2. In the **Address/Mask** field, enter the IP address and mask of the subnet for which you want to configure the network route.
3. If you want to use the default network route, enter 0.0.0.0/0.
4. In the **Gateway** field, enter the IP address of the gateway.
5. Click **Ok**.
6. If you want to add other network routes, repeat the steps in the **IPv4 Static Route** window.
7. If you are done adding network routes, click **Continue**.

The Setup Wizard proceeds to the next step.

# Step 8. Configuring the minimum password length for the Sandbox administrator password

*To set the minimum length of the administrator password for the Sandbox component:*

1. In the **Minimal length**, enter the length in characters. Passwords 12 or more characters long are recommended.
2. Click **Ok**.

The Setup Wizard proceeds to the next step.

# Step 9. 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**.

   This opens a window with the IP address of the Sandbox server. You can enter this address in your web browser to open the Sandbox web interface. To log in, use the Sandbox administrator account that you have created.

   The Sandbox server will restart.

Proceed to configuration of the Sandbox component through the web interface.

# 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**.

   This opens the settings window.
6. On the **Ports** tab, select the **VM Network** section.

   This opens the **VM Network Properties** window.
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.

*To begin installing the Central Node and Sensor components:*

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.

   This opens the program installation start window.

3. Click **Ok**.

# 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** and press **ENTER**.

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

2. Please read the End User License Agreement.

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

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

4. Please carefully read the Privacy Policy.

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

The Setup Wizard proceeds to the next step.

# Step 2. 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. This opens the **Select action** window.

4. Select **Install**.
5. Press **ENTER**.

   This opens a window displaying a warning that the disk will be formatted.
6. Click **Install**.

The disk will be formatted. The server is restarted.

The Setup Wizard proceeds to the next step.

# Step 3. Selecting a server role

*To select the server role:*

1. 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.
2. This opens the confirmation window for your server role selection.

   Click **Confirm role**.

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

# Step 4. Configuring the minimum password length for the administrator password

*To set the minimum length of the administrator password:*

1. In the **Minimal length**, enter the length in characters. Passwords 12 or more characters long are recommended.
2. Click **Ok**.

The Setup Wizard proceeds to the next step.

# Step 5. 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 6. Assigning the host name

At this step, assign a server host name to be used by DNS servers.

*To assign a server host name:*

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 7. 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 8. Assigning the address and subnet mask of the management interface

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

1. Select **IP addr** and press **ENTER**.

   This opens the window for entering an IP address and a subnet mask.
2. In the **Address** field, enter the IP address that you want to assign to this network interface.
3. In the **Netmask** field, enter the subnet mask in which you want to use this network interface.
4. Click **Ok**.

   The window for entering an IP address and a subnet mask is closed.
5. Select **Go Back** and press **ENTER**.

   The network interface settings window is closed.
6. Select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 9. Configuring the default network route

*To configure the default network route for the application:*

1. In the **Default route** list, select **Interface** and press **ENTER**.

   This opens the list of network interfaces.

2. Select the network interface for which you want to configure the network route and press **ENTER**.

   The Setup Wizard returns to the network route configuration window.

3. Select **Gateway** and press **ENTER**.

   This opens the window for entering a static gateway address.

4. Enter a static gateway address into the **Gateway** field.

5. 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.

6. Select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 10. Configuring DNS settings

During this step, configure the DNS settings for the operation of servers with program components.

*To assign static DNS addresses:*

1. In the **Select action - Resolver** window, select any setting (for example, **Search list**) and press **ENTER**.

   This opens the window for entering static DNS addresses.

2. In the **Search list** field, enter the DNS suffix that you want to use in Kaspersky Anti Targeted Attack Platform. For example: example.com.

3. In the **Primary** field, enter the IP address of the primary DNS server in IPv4 format.

4. In the **Secondary** field, enter the IP address of the secondary DNS server in IPv4 format.

5. Click **Ok**.

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

6. Verify that the DNS settings are correct.

7. Select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 11. 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 setting (for example, **Host**) and press **ENTER**.

   This opens a window for configuring proxy server connection settings.

2. 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

3. 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 12. 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, **Russia**) and press **ENTER**.

   This displays a list of time zones available for the selected country.
2. Select the time zone and press **ENTER**.

   This opens a window for confirming the time zone selection.
3. If the time zone has been correctly selected, click **Yes**.

The Setup Wizard proceeds to the next step.

# Step 13. 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**.

   This opens the **Configure NTP servers** window.

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 14. Configuring integration 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.

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.

# Step 15. 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**.

   This opens the action confirmation window.
3. Click **Yes**.

The server is restarted.

The Setup Wizard proceeds to the next step.

# Step 16. Creating an administrator account for the web interface of Kaspersky Anti Targeted Attack Platform

*To create an 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 17. Configuring receipt of mirrored traffic from SPAN ports

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

*To turn off 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:*

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

This opens the window with settings for receiving mirrored traffic from SPAN ports.

## Selecting network interfaces for receiving mirrored traffic from SPAN ports

*To select network interfaces for receiving mirrored traffic from SPAN ports:*

1. In the **Select action** window, select **Setup capture interfaces** and press **ENTER**.

   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 for which you want to receive mirrored traffic and press **ENTER**.

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

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.

If you want to configure receipt of mirrored traffic for other network interfaces, repeat the step for each of them. One network interface must keep the **skip** value.

3. Select **Go Back** and press **ENTER**.

## Selecting network protocols for receiving mirrored traffic from SPAN ports

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

1. In the **Select action** window, select **Setup capture protocols** and press **ENTER**.

   This opens a window for selecting network protocols.

   - **dns**
   - **ftp**
   - **http**
   - **smtp**

   By default, receipt of mirrored traffic from SPAN ports is enabled for all network protocols. The value **on** is displayed to the right of the names of the network protocols.

2. If you want to disable the receipt of mirrored traffic from SPAN ports for a particular protocol, select the protocol and press **ENTER**.

   Example:
   If you configured the integration with a mail server via SMTP, all SMTP traffic of your company passes through that mail server and you do not need to additionally scan SMTP traffic on the proxy server; you can disable the receipt of mirrored traffic from SPAN ports over SMTP.

   Receipt of mirrored traffic from SPAN ports over the selected protocol is disabled. The value **off** is displayed to the right of the name of the network interface.

3. If you want to disable the receipt of mirrored traffic from SPAN ports over other protocols or re-enable the receipt of mirrored traffic, repeat the step.

4. Select **Go Back** and press **ENTER**.

## Configuring the transmission of HTTP traffic details for IDS alerts

*To configure the transmission of HTTP traffic details (HTTP body) for IDS alerts:*

1. In the **Select action** window, select **Setup http-body dump** and press **ENTER**.

   By default, the transmission of HTTP traffic details for IDS alerts is enabled. The value **yes** is displayed to the right of the **http-body enabled** setting.

2. If you want to disable the transmission of HTTP traffic details for IDS alerts (for example, to reduce the burden on the system), select **http-body enabled** and press **ENTER**.

   The value **off** is displayed to the right of the **http-body enabled** setting. IDS alerts no longer display the "HTTP body" field.

3. If you want to re-disable the transmission of HTTP traffic details for IDS alerts, repeat the step.

4. Select **Continue** and press **ENTER**.

5. In the **Select action** window, select **Continue.** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 18. 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.

If you use a separate proxy server, by default, Kaspersky Anti Targeted Attack Platform does not encrypt ICAP traffic or authenticate ICAP clients. The application administrator must independently ensure a secure network connection between your proxy server and Kaspersky Anti Targeted Attack Platform by using traffic tunneling or iptables.

*To turn off the integration of Kaspersky Anti Targeted Attack Platform 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 19. 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.

*To turn off the 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**.

    This opens the **Cipher list** window.

    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 20. 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**.

   This opens the **Configure Networks** window.

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**.

   This opens the **Configure domains** window.

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**.

    This opens the **Select TLS encryption level** window.

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**.

    This opens the **Select TLS client certificates use** window.

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**.

    This opens the **Message size limit** window.

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**.

Installation is complete.

# 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**.

   This opens the settings window.
6. On the **Ports** tab, select the **VM Network** section.

   This opens the **VM Network Properties** window.
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.

*To begin installing the Sensor component:*

1. Run the disk image containing the Central Node and Sensor components.

   The Setup Wizard starts.
2. Click **Ok**.

# 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** and press **ENTER**.

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

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

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

4. Please carefully read the Privacy Policy.

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

The Setup Wizard proceeds to the next step.

# Step 2. Selecting a disk for installing the Sensor component

At this step, select a physical 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 and press **ENTER**.

2. This opens the **Select action** window.

3. Select **Install** and press **ENTER**.

   If the disk is not empty, a window is displayed asking you to confirm that you want to format the disk and install the program.

4. Click **Install**.

   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. Selecting a server role

*To select the server role:*

1. Select **Act as Sensor**.

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

   Click **Confirm role**.

This starts the setup wizard for the Sensor component.

# Step 4. Configuring the minimum password length for the administrator password

*To set the minimum length of the administrator password:*

1. In the **Minimal length**, enter the length in characters. Passwords 12 or more characters long are recommended.
2. Click **Ok**.

The Setup Wizard proceeds to the next step.

# Step 5. 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 6. Assigning the host name

At this step, assign a server host name to be used by DNS servers.

*To assign a server host name:*

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 7. 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 8. Assigning the address and subnet mask of the management interface

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

1. Select **IP addr** and press **ENTER**.

   This opens the window for entering an IP address and a subnet mask.

2. In the **Address** field, enter the IP address that you want to assign to this network interface.

3. In the **Netmask** field, enter the subnet mask in which you want to use this network interface.

4. Click **Ok**.

   The window for entering an IP address and a subnet mask is closed.

5. Select **Go Back** and press **ENTER**.

   The network interface settings window is closed.

6. Select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 9. Configuring the default network route

*To configure the default network route for the application:*

1. In the **Default route** list, select **Interface** and press **ENTER**.

   This opens the list of network interfaces.

2. Select the network interface for which you want to configure the network route and press **ENTER**.

   The Setup Wizard returns to the network route configuration window.

3. Select **Gateway** and press **ENTER**.

   This opens the window for entering a static gateway address.

4. Enter a static gateway address into the **Gateway** field.

5. 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.

6. Select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 10. Configuring DNS settings

During this step, configure the DNS settings for the operation of servers with program components.

*To assign static DNS addresses:*

1. In the **Select action - Resolver** window, select any setting (for example, **Search list**) and press **ENTER**.

   This opens the window for entering static DNS addresses.

2. In the **Search list** field, enter the DNS suffix that you want to use in Kaspersky Anti Targeted Attack Platform. For example: example.com.

3. In the **Primary** field, enter the IP address of the primary DNS server in IPv4 format.

4. In the **Secondary** field, enter the IP address of the secondary DNS server in IPv4 format.

5. Click **Ok**.

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

6. Verify that the DNS settings are correct.
7. Select **Continue** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 11. 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 setting (for example, **Host**) and press **ENTER**.

   This opens a window for configuring proxy server connection settings.
2. 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
3. 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 12. 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, **Russia**) and press **ENTER**.

   This displays a list of time zones available for the selected country.
2. Select the time zone and press **ENTER**.

   This opens a window for confirming the time zone selection.
3. If the time zone has been correctly selected, click **Yes**.

The Setup Wizard proceeds to the next step.

# Step 13. 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**.
   This opens the **Configure NTP servers** window.
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 14. 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**.
   This opens the **Central Node certificate** window.

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**.

   This opens the **Central Node connection** window.

   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. 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 15. 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 16. Configuring receipt of mirrored traffic from SPAN ports

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

*To turn off 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:*

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

This opens the window with settings for receiving mirrored traffic from SPAN ports.

## Selecting network interfaces for receiving mirrored traffic from SPAN ports

*To select network interfaces for receiving mirrored traffic from SPAN ports:*

1. In the **Select action** window, select **Setup capture interfaces** and press **ENTER**.

   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 for which you want to receive mirrored traffic and press **ENTER**.

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

   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.

   If you want to configure receipt of mirrored traffic for other network interfaces, repeat the step for each of them. One network interface must keep the **skip** value.

3. Select **Go Back** and press **ENTER**.

## Selecting network protocols for receiving mirrored traffic from SPAN ports

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

1. In the **Select action** window, select **Setup capture protocols** and press **ENTER**.

   This opens a window for selecting network protocols.

   - **dns**
   - **ftp**
   - **http**
   - **smtp**

   By default, receipt of mirrored traffic from SPAN ports is enabled for all network protocols. The value **on** is displayed to the right of the names of the network protocols.

2. If you want to disable the receipt of mirrored traffic from SPAN ports for a particular protocol, select the protocol and press **ENTER**.

   > Example:
   > If you configured the integration with a mail server via SMTP, all SMTP traffic of your company passes through that mail server and you do not need to additionally scan SMTP traffic on the proxy server; you can disable the receipt of mirrored traffic from SPAN ports over SMTP.

   Receipt of mirrored traffic from SPAN ports over the selected protocol is disabled. The value **off** is displayed to the right of the name of the network interface.

3. If you want to disable the receipt of mirrored traffic from SPAN ports over other protocols or re-enable the receipt of mirrored traffic, repeat the step.

4. Select **Go Back** and press **ENTER**.

## Configuring the transmission of HTTP traffic details for IDS alerts

*To configure the transmission of HTTP traffic details (HTTP body) for IDS alerts:*

1. In the **Select action** window, select **Setup http-body dump** and press **ENTER**.

   By default, the transmission of HTTP traffic details for IDS alerts is enabled. The value **yes** is displayed to the right of the **http-body enabled** setting.

2. If you want to disable the transmission of HTTP traffic details for IDS alerts (for example, to reduce the burden on the system), select **http-body enabled** and press **ENTER**.

   The value **off** is displayed to the right of the **http-body enabled** setting. IDS alerts no longer display the "HTTP body" field.

3. If you want to re-disable the transmission of HTTP traffic details for IDS alerts, repeat the step.

4. Select **Continue** and press **ENTER**.

5. In the **Select action** window, select **Continue.** and press **ENTER**.

The Setup Wizard proceeds to the next step.

# Step 17. 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.

If you use a separate proxy server, by default, Kaspersky Anti Targeted Attack Platform does not encrypt ICAP traffic or authenticate ICAP clients. The application administrator must independently ensure a secure network connection between your proxy server and Kaspersky Anti Targeted Attack Platform by using traffic tunneling or iptables.

*To turn off the integration of Kaspersky Anti Targeted Attack Platform 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 18. 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.

*To turn off the 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**.

    This opens the **Cipher list** window.

    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 19. 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**.

   This opens the **Configure Networks** window.

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**.

   This opens the **Configure domains** window.

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**.

    This opens the **Select TLS encryption level** window.

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**.

    This opens the **Select TLS client certificates use** window.

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**.

    This opens the **Message size limit** window.

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**.

Installation is complete.

# Configuring the integration of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent

This section contains information on configuring the integration of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent. You must follow the steps both on the Kaspersky Anti Targeted Attack Platform side using the web interface and program administrator menu and on the Kaspersky Endpoint Agent side using the KSC Administration Console.

## Configuring the trusted connection of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent

You must configure a trusted connection of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent both on the Kaspersky Anti Targeted Attack Platform side using the web interface and program administrator menu and on the Kaspersky Endpoint Agent side using the KSC Administration Console.

You can use one of the following options to configure a trusted connection:

1. Using a TLS certificate of Kaspersky Anti Targeted Attack Platform. Without validating the Kaspersky Endpoint Agent TLS certificate on the Kaspersky Anti Targeted Attack Platform side.

   a. Configuring the connection with the Central Node server without validating the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

      Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Central Node server. Kaspersky Anti Targeted Attack Platform does not validate the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

   b. Configuring the connection with the Sensor server without validating the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

      Traffic redirection to the Sensor server is configured in Kaspersky Anti Targeted Attack Platform. Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Sensor server. Kaspersky Anti Targeted Attack Platform does not validate the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

2. Using TLS certificates of Kaspersky Anti Targeted Attack Platform and Kaspersky Endpoint Agent. Validating the Kaspersky Endpoint Agent TLS certificate on the Kaspersky Anti Targeted Attack Platform side.

   a. Configuring the connection with the Central Node server with validation of the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

      Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Central Node server. Additional security of the connection is configured in Kaspersky Endpoint Agent and the TLS certificate of Kaspersky Endpoint Agent is uploaded. Kaspersky Anti Targeted Attack Platform validates the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

b. Configuring the connection with the Sensor server with validation of the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

Traffic redirection to the Sensor server is configured in Kaspersky Anti Targeted Attack Platform. Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Sensor server. Additional security of the connection is configured in Kaspersky Endpoint Agent and the TLS certificate of Kaspersky Endpoint Agent is uploaded. Kaspersky Anti Targeted Attack Platform validates the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

# Configuring the connection with the Central Node server without validating the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Central Node server. Kaspersky Anti Targeted Attack Platform does not validate the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

If you are using this alternative configuration for the trusted connection, the procedure is as follows:

1. **Generate or upload an independently prepared TLS certificate of the Central Node server in the web interface of Central Node (if the TLS certificate of the Central Node is not created yet).**
2. **Downloading the TLS certificate of the Central Node server to your computer**
3. **Uploading the TLS certificate of the Central Node server to Kaspersky Endpoint Agent using the KSC Administration Console.**

# Configuring the connection with the Sensor server without validating the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

Traffic redirection to the Sensor server is configured in Kaspersky Anti Targeted Attack Platform. Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Sensor server. Kaspersky Anti Targeted Attack Platform does not validate the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

If you are using this alternative configuration for the trusted connection, the procedure is as follows:

1. **Enabling traffic redirection from Kaspersky Endpoint Agent to the Sensor server.**
2. **Authorizing the Sensor component on the Central Node server.**
3. **Generating or uploading an independently prepared TLS certificate for the Sensor server in the administrator menu of the Sensor server.**
4. **Downloading the TLS certificate of the Sensor server to your computer.**
5. **Uploading the TLS certificate of the Sensor server to Kaspersky Endpoint Agent using the KSC Administration Console.**

# Configuring the connection with the Central Node server with validation of the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Central Node server. Additional security of the connection is configured in Kaspersky Endpoint Agent and the TLS certificate of Kaspersky Endpoint Agent is uploaded. Kaspersky Anti Targeted Attack Platform validates the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

If you are using this alternative configuration for the trusted connection, the procedure is as follows:

1. **Generate or upload an independently prepared TLS certificate of the Central Node server in the web interface of Central Node (if the TLS certificate of the Central Node is not created yet).**
2. **Downloading the TLS certificate of the Central Node server to your computer**
3. **Uploading the TLS certificate of the Central Node server to Kaspersky Endpoint Agent using the KSC Administration Console.**
4. **Enabling the validation of the Kaspersky Endpoint Agent TLS certificate in the web interface of Kaspersky Anti Targeted Attack Platform.**
5. **Generating and downloading the cryptographic container with the TLS certificate of Kaspersky Endpoint Agent or uploading an independently prepared TLS certificate of Kaspersky Endpoint Agent using the web interface of Kaspersky Anti Targeted Attack Platform.**

   If you want to prepare the TLS certificate of Kaspersky Endpoint Agent on your own, you must create a PFX cryptographic container with your certificate. For details on managing TLS certificates, see the OpenSSL documentation.

6. **Uploading the cryptographic container with Kaspersky Endpoint Agent certificate to Kaspersky Endpoint Agent using the KSC Administration Console.**

# Configuring the connection with the Sensor server with validation of the TLS certificate of Kaspersky Endpoint Agent in Kaspersky Anti Targeted Attack Platform.

Traffic redirection to the Sensor server is configured in Kaspersky Anti Targeted Attack Platform. Kaspersky Endpoint Agent establishes a trusted connection with Kaspersky Anti Targeted Attack Platform using the TLS certificate of the Sensor server. Additional security of the connection is configured in Kaspersky Endpoint Agent and the TLS certificate of Kaspersky Endpoint Agent is uploaded. Kaspersky Anti Targeted Attack Platform validates the TLS certificate of Kaspersky Endpoint Agent when Kaspersky Endpoint Agent tries to connect.

If you are using this alternative configuration for the trusted connection, the procedure is as follows:

1. Enabling traffic redirection from Kaspersky Endpoint Agent to the Sensor server.
2. Authorizing the Sensor component on the Central Node server.
3. Generating or uploading an independently prepared TLS certificate for the Sensor server in the administrator menu of the Sensor server.
4. Downloading the TLS certificate of the Sensor server to your computer.
5. Uploading the TLS certificate of the Sensor server to Kaspersky Endpoint Agent using the KSC Administration Console.
6. Enabling the validation of the Kaspersky Endpoint Agent TLS certificate in the web interface of Kaspersky Anti Targeted Attack Platform.
7. Generating and downloading the cryptographic container with the TLS certificate of Kaspersky Endpoint Agent or uploading an independently prepared TLS certificate of Kaspersky Endpoint Agent using the web interface of Kaspersky Anti Targeted Attack Platform.

   If you want to prepare the TLS certificate of Kaspersky Endpoint Agent on your own, you must create a PFX cryptographic container with your certificate. For details on managing TLS certificates, see the OpenSSL documentation.

8. Uploading the cryptographic container with Kaspersky Endpoint Agent certificate to Kaspersky Endpoint Agent using the KSC Administration Console.

# Downloading the TLS certificate of the Central Node server

*To download the TLS certificate to your computer:*

1. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **General settings** subsection.
2. In the **TLS certificate** settings group, click the **Download** button.

The server certificate file will be saved in the downloads folder of the browser.

# Generating a TLS certificate for the Central Node server in the web interface of Kaspersky Anti Targeted Attack Platform

If you are already using a Central Node server TLS certificate, generating a new certificate causes the currently used certificate to be removed and replaced with the newly generated certificate.

You must enter the data of the new certificate everywhere the old certificate was used.

If you replace the TLS certificate, you will need to:

- Reauthorize mail sensors (KSMG, KLMS) on Central Node.
- Reconfigure connection of Central Node, PCN and SCN to Sandbox.
- Reconfigure Endpoint Agent traffic redirection to Sensor and trusted connection with Endpoint Agent.
- Upload a new certificate in Active Directory (if you use Active Directory).

Please delete all Endpoint Agent host isolation rules. Connection with the isolated hosts and control over them will be lost.

*To generate a TLS certificate for the Central Node server:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **General settings** subsection.
3. In the **TLS certificate** settings group, click the **Generate** button.

   This opens the action confirmation window.
4. Click **Yes**.

Kaspersky Anti Targeted Attack Platform generates a new TLS certificate. The page is automatically refreshed.

# Uploading an independently prepared TLS certificate for the Central Node server using the web interface of Kaspersky Anti Targeted Attack Platform.

You can choose to prepare the TLS certificate on your own and upload it using the Kaspersky Anti Targeted Attack Platform web interface.

The TLS certificate file prepared for upload 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 private key length must be 2048 bits or longer.

For more details on preparing TLS certificates for import, please refer to the documentation on Open SSL.

If you are already using a Central Node server TLS certificate, uploading a new certificate causes the currently used certificate to be removed and replaced with the uploaded certificate.

You must enter the data of the new certificate everywhere the old certificate was used.

If you replace the TLS certificate, you will need to:

- Reauthorize mail sensors (KSMG, KLMS) on Central Node.
- Reconfigure connection of Central Node, PCN and SCN to Sandbox.
- Reconfigure Endpoint Agent traffic redirection to Sensor and trusted connection with Endpoint Agent.
- Upload a new certificate in Active Directory (if you use Active Directory).

Please delete all Endpoint Agent host isolation rules. Connection with the isolated hosts and control over them will be lost.

*To upload an independently prepared TLS certificate using the Kaspersky Anti Targeted Attack Platform web interface:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **General settings** subsection.
3. In the **TLS certificate** settings group, click the **Upload** button.

   This opens the file selection window.

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

   This closes the file selection window.

The TLS certificate is added to the Kaspersky Anti Targeted Attack Platform.

# Uploading a TLS certificate of the Central Node server or Sensor to Kaspersky Endpoint Agent

*To upload a TLS certificate of the Central Node or Sensor server to Kaspersky Endpoint Agent:*

1. Open the KSC Console.
2. In the console tree, open the **Policies** folder.
3. In the Kaspersky Endpoint Agent policy section, select the required policy and double-click it to open its properties.

   The properties of the selected policy are displayed.
4. In the **KATA integration** section, select the **KATA Central Node** subsection.
5. Select the **Enable KATA integration** check box.
6. In the **Address** field, enter the address of the Central Node server of the Kaspersky Anti Targeted Attack Platform program that you want to configure integration with, and select a port to use for the connection. Port 443 is used by default.
7. Select the **Use trusted connection** check box.
8. Click **Add new TLS certificate**.

   The **Adding TLS certificate** window opens.
9. To add a TLS certificate previously created on the Kaspersky Anti Targeted Attack Platform side and downloaded, do one of the following:

   - Add a certificate file. To do so, click **Browse**; in the window that opens, select a certificate file and click **Open**.
   - Paste the contents of the certificate file into the **OR** field.

   Kaspersky Endpoint Agent can store only one TLS certificate for the Kaspersky Anti Targeted Attack Platform server. If you have added a TLS certificate before and are adding a TLS certificate again, only the last added certificate is used.

   If you have configured traffic redirection to the server with the Sensor component, you must download the TLS certificate of the Sensor server and then upload it here.
10. Click **Add**.

Information about the added TLS certificate is displayed in the section for integration with Kaspersky Anti Targeted Attack Platform.

11. In the upper right corner of the settings group, switch from **Unaffected by policy** to **Under policy**.

12. Click **OK**.

The TLS certificate of the Central Node server is uploaded to Endpoint Agent.

# Enabling the validation of the Kaspersky Endpoint Agent TLS certificate in the web interface of Kaspersky Anti Targeted Attack Platform

*To enable the trusted connection with Kaspersky Endpoint Agent:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.

2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **Endpoint Agent certificates** subsection.

3. Turn on the **Validate Endpoint Agent TLS certificates** switch.

Kaspersky Anti Targeted Attack Platform will check TLS certificate data when Kaspersky Endpoint Agent attempts to connect to Kaspersky Anti Targeted Attack Platform.

# Generating a TLS certificate of Kaspersky Endpoint Agent in the web interface of Kaspersky Anti Targeted Attack Platform and downloading a cryptographic container

*To generate a TLS certificate for the connection of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.

2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **Endpoint Agent certificates** subsection.

3. Click **Generate**.

Kaspersky Anti Targeted Attack Platform generates a new TLS certificate. The page is automatically refreshed.

The cryptographic container fine with the Kaspersky Endpoint Agent certificate in the PFX format is downloaded to the browser downloads folder on your local computer.

You can use the cryotographic container to configure the validation of Kaspersky Endpoint Agent TLS certificate by the Central Node server when attempting to connect to Kaspersky Anti Targeted Attack Platform.

By default, the cryptographic container is not password-protected. You can protect the cryptographic container with a password. For details on managing TLS certificates, see the OpenSSL documentation.

The cryptographic container contains only the certificate file, but not the private key file. Kaspersky Anti Targeted Attack Platform does not store private keys for the TLS encryption of the connection.

# Uploading an independently prepared TLS certificate of Kaspersky Endpoint Agent using the web interface of Kaspersky Anti Targeted Attack Platform.

You can choose to prepare the TLS certificate on your own and upload it using the Kaspersky Anti Targeted Attack Platform web interface.

The TLS certificate file prepared for upload 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 private key length must be 2048 bits or longer.

For more details on preparing TLS certificates for import, please refer to the documentation on Open SSL.

If you want to prepare the TLS certificate of Kaspersky Endpoint Agent on your own, you must create a PFX cryptographic container with your certificate and upload the cryptographic container to Kaspersky Endpoint Agent.

You can use the cryotographic container to configure the validation of Kaspersky Endpoint Agent TLS certificate by the Central Node server when attempting to connect to Kaspersky Anti Targeted Attack Platform.

For details on managing TLS certificates, see the OpenSSL documentation.

The cryptographic container must contain only the certificate file, but not the private key file. Kaspersky Anti Targeted Attack Platform does not store private keys for the TLS encryption of the connection.

*To upload an independently prepared TLS certificate of Kaspersky Endpoint Agent using the Kaspersky Anti Targeted Attack Platform web interface:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **Endpoint Agent certificates** subsection.
3. Click **Upload**.

   This opens the file selection window.

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

   This closes the file selection window.

The TLS certificate is added to the Kaspersky Anti Targeted Attack Platform.

# Viewing the table of Kaspersky Endpoint Agent TLS certificates in the web interface of Kaspersky Anti Targeted Attack Platform

*To view the list of TLS certificates for connection with Kaspersky Endpoint Agent using the Kaspersky Anti Targeted Attack Platform web interface:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **Endpoint Agent certificates** subsection.
3. The list of TLS certificates opens with the following information for each certificate:
   - **TLS certificate** – Fingerprint of the certificate.
   - **Serial number** —Serial number of the certificate.
   - **Expires** —Expiration date of the certificate.

# Filtering and searching Kaspersky Endpoint Agent TLS certificates in the web interface of Kaspersky Anti Targeted Attack Platform

You can filter TLS certificate displayed in the table by one or both columns (**TLS certificate** and **Serial number**) or enter search criteria to search TLS certificates by these columns.

*To filter and search TLS certificates in the table:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **Endpoint Agent certificates** subsection.
3. The list of TLS certificates opens with the following information for each certificate:
   - **TLS certificate** – Fingerprint of the certificate.
   - **Serial number** —Serial number of the certificate.
   - **Expires** —Expiration date of the certificate.

4. If you want to filter or search TLS certificates by certificate fingerprint:

    a. Click the **TLS certificate** link to open the filter configuration window.

    b. In the **TLS certificate** text box, enter a few characters of the certificate fingerprint.

    c. Click **Apply**.

5. If you want to filter or search TLS certificates by serial number:

    a. Click the **Serial number** link to open the filter configuration window.

    b. In the **Serial number** text box, enter a few characters of the serial number.

    c. Click **Apply**.

The table displays only those TLS certificates that match the filter criteria you have set.

*To clear the filter for one or more filtering criteria:*

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.

# Deleting Kaspersky Endpoint Agent TLS certificates in the web interface of Kaspersky Anti Targeted Attack Platform

*To delete one or more TLS certificates for connection with Kaspersky Endpoint Agent using the Kaspersky Anti Targeted Attack Platform web interface:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **Endpoint Agent certificates** subsection.
3. The table of TLS certificates opens.
4. Select check boxes next to one or more TLS certificates that you want to delete.

5. Click **Delete**.

   This opens the action confirmation window.

6. Click **Yes**.

The selected TLS certificates are deleted.

# Configuring the validation of the Kaspersky Endpoint Agent TLS certificate by the Central Node server and uploading a cryptographic container to Kaspersky Endpoint Agent

*To configure the validation of Kaspersky Endpoint Agent TLS certificate by the Central Node server and upload the cryptographic container with the Kaspersky Endpoint Agent certificate to Kaspersky Endpoint Agent:*

1. Open the KSC Console.
2. In the console tree, open the **Policies** folder.
3. In the Kaspersky Endpoint Agent policy section, select the required policy and double-click it to open its properties.

   The properties of the selected policy are displayed.

4. In the **KATA integration** section, select the **KATA Central Node** subsection.
5. Click **Configure additional security**.
6. In the window that opens, select the **Secure the connection with client certificate** check box.
7. Click **Upload**.

   This opens the file selection window on your local computer.

8. Select the cryptographic container file of the Kaspersky Endpoint Agent certificate that was generated on the Kaspersky Anti Targeted Attack Platform server and downloaded to the hard drive of your computer.
9. Click **OK**.

   The window closes.

10. In the upper right corner of the settings group, switch from **Unaffected by policy** to **Under policy**.
11. Click **OK**.

The cryptographic container with the Kaspersky Endpoint Agent certificate is uploaded to Kaspersky Endpoint Agent. Kaspersky Anti Targeted Attack Platform now validates the TLS certificate of Kaspersky Endpoint Agent when it tries to connect.

# Configuring traffic redirection from Kaspersky Endpoint Agent to the Sensor server

You can use the server hosting the Sensor component as a proxy server during data exchange between the Kaspersky Endpoint Agent program and the Central Node component to decrease the load 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 Kaspersky Endpoint Agent is 1000.
- 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.

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 are using the Sensor component as a proxy server, make sure to enter the IP address of the Sensor component instead of the IP address of Central Node when configuring the integration of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent on the Kaspersky Endpoint Agent side.

# Enabling and disabling traffic redirection from Kaspersky Endpoint Agent to the Sensor server

*To enable or disable using the Sensor component as a proxy server for communication between Kaspersky Endpoint Agent and the Central Node component, do the following in the administrator menu of the server hosting the Sensor component:*

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 Central Node server

*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:*

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.

   This opens the authorization confirmation window.

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.

# Generating a TLS certificate for the Sensor server in the administrator menu of the Sensor server

*To create a TLS certificate for the server with the Sensor component, do the following in the administrator menu of the Sensor server:*

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**.

   This opens the **Certificate management** window.
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 **Continue**.

   This opens the action confirmation window.
8. Click **Generate**.

   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 **Continue**.

    This opens the action confirmation window.
11. Click **Ok**.

The certificate will be created. The data of previously installed certificates will be overwritten.

# Uploading an independently prepared TLS certificate for the Sensor server in the administrator menu of the Sensor server

You can independently prepare a TLS certificate and upload it to the server with the Sensor component via the SCP protocol. For more details on the methods for uploading files via the SCP protocol, see the documentation for the operating system installed on the computer from which you want to upload the TLS certificate.

The TLS certificate file prepared for upload to the server 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 TLS certificates for import, please refer to the documentation on Open SSL.

*To upload an independently prepared TLS certificate to the server with the Sensor 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. Run the following command: `scp kata.pem admin@<IP address of the server with the Sensor component>:`
2. At the password prompt, enter the administrator password for working in the administrator menu of the server with the Sensor component that was set during installation.

The TLS certificate is uploaded to the server with the Sensor component.

*To apply the uploaded TLS certificate on the server with the Sensor component, do the following in the administrator menu of the Sensor server:*

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**.

   This opens the **Certificate management** window.
5. In the lower part of the window, select **kata.pem**.
6. Press **ENTER**.

   This opens the **Uploaded certificate** window.

7. Select **Install certificate**.
8. Press **ENTER**.

   This opens the action confirmation window.
9. Click **Yes**.

   This opens a window containing information about the certificate.
10. Click **Continue**.

    This opens the action confirmation window.
11. Click **Install**.

    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 **Continue**.

    This opens the action confirmation window.
14. Click **Ok**.

The certificate will be applied. The data of previously installed certificates will be overwritten.

# Downloading the TLS certificate of the Sensor server to your computer

You can download a TLS certificate from the Sensor server to any computer that can connect to the Sensor server over the SCP protocol. For more details on the methods for uploading files via the SCP protocol, see the documentation for the operating system installed on the computer to which you want to download the TLS certificate.

*To download the TSL certificate from the server with the Sensor component over the SCP protocol, do the following in your computer's interface used for working over the SCP protocol (using the Linux operating system as an example):*

1. Run the following command: `scp admin@<IP address of the server with the Sensor component>:ssl/kata.crt .`
2. At the password prompt, enter the administrator password for working in the administrator menu of the server with the Sensor component that was set during installation.

The TLS certificate is downloaded from the server with the Sensor component to the current folder.

# Configuring the integration and trusted connection with Kaspersky Anti Targeted Attack Platform on the Kaspersky Endpoint Agent side

*To configure the integration with Kaspersky Anti Targeted Attack Platform on the Kaspersky Endpoint Agent side:*

1. Open the KSC Console.
2. In the console tree, open the **Policies** folder.
3. In the Kaspersky Endpoint Agent policy section, select the required policy and double-click it to open its properties.

   The properties of the selected policy are displayed.
4. In the **KATA integration** section, select the **KATA Central Node** subsection.
5. Select the **Enable KATA integration** check box.
6. In the **Address** field, enter the address of the Central Node server of the Kaspersky Anti Targeted Attack Platform program that you want to configure integration with, and select a port to use for the connection. Port 443 is used by default.
7. Select the **Use trusted connection** check box.
8. Click **Add new TLS certificate**.

   The **Adding TLS certificate** window opens.
9. To add a TLS certificate previously created on the Kaspersky Anti Targeted Attack Platform side and downloaded, do one of the following:

   - Add a certificate file. To do so, click **Browse**; in the window that opens, select a certificate file and click **Open**.
   - Paste the contents of the certificate file into the **OR** field.

   Kaspersky Endpoint Agent can store only one TLS certificate for the Kaspersky Anti Targeted Attack Platform server. If you have added a TLS certificate before and are adding a TLS certificate again, only the last added certificate is used.

   If you have configured traffic redirection to the server with the Sensor component, you must download the TLS certificate of the Sensor server and then upload it here.
10. Click **Add**.

    Information about the added TLS certificate is displayed in the section for integration with Kaspersky Anti Targeted Attack Platform.
11. Click **Configure additional security**.

12. In the window that opens, select the **Secure the connection with client certificate** check box.

13. Click **Upload**.

    This opens the file selection window on your local computer.

14. Select the cryptographic container file of the Kaspersky Endpoint Agent certificate that was generated on the Kaspersky Anti Targeted Attack Platform server and downloaded to the hard drive of your computer.

15. Click **OK**.

    The window closes.

16. In the **Timeout** field, enter the maximum response timeout of the Kaspersky Anti Targeted Attack Platform Central Node server in minutes.

17. In the **Send synchronization request to the KATA server every...** field, enter the period in minutes.

18. If you want Kaspersky Endpoint Agent to look for data on previous object scans in the cache before sending objects for scanning to Kaspersky Anti Targeted Attack Platform, select the **Use event cache** check box and enter the storage period for object scan results in the cache in seconds.

19. In the upper right corner of the settings group, switch from **Unaffected by policy** to **Under policy**.

20. Click **OK**.

The integration with Kaspersky Anti Targeted Attack Platform on the Kaspersky Endpoint Agent side is configured.

# 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.

For each user account, the number of simultaneous program management sessions is limited to one IP address. If the same user name is used to sign in to the program from a different IP address, the earlier session is terminated.

# 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.

Make sure that access to Kaspersky Anti Targeted Attack Platform administrator menu and server management console is possible only from computers to which you have granted such access.

Make sure the computers to which you grant access are inside the secure perimeter of your network.

You can configure access to Kaspersky Anti Targeted Attack Platform administrator menu and server management console from certain computers using the iptables command-line utility. For detailed information about managing iptables, see the iptables documentation.

*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 user name and the password that was specified during installation of the program.

   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 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. Such files are retained indefinitely and can be manually deleted by the administrator of Kaspersky Anti Targeted Attack Platform. The path for trace files is specified by the administrator of Kaspersky Anti Targeted Attack Platform.

*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 user name and the password that was specified during installation of the program.

   The program component administrator menu is displayed.
3. In the program administrator menu, select **Technical Support Mode**.
4. Press **ENTER**.

   This opens the Technical Support Mode confirmation window.
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 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 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 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.

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 **Cluster management** 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. 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.

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.<br>It is not possible to use a link on the widget to go to the **Alerts** section. |
| **Alerts** | The following actions are not available:<br>• Viewing information about an alert.<br>• Marking the completion of VIP group alert processing.<br>• Performing operations on multiple alerts.<br>• 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. |
| **User rules** | Read access. |
| **Storage** | There is no access to objects that are placed in Storage as a result of tasks.<br>Full access to objects that were manually downloaded by the user. |
| **Endpoint Agents** | Access to view tables of computers with the Endpoint Agent component, and restrictions on viewing data on tasks, policies, and network isolation. |
| Network isolation of hosts | No access. |
| **Reports** | No access. |
| **Program settings: IOC scanning schedule** | Read access. |
| **Program settings: Endpoint Agents** | Read access. |
| **Program settings: KPSN reputation database** | No access. |
| **Program settings: Notifications** | No access to rules for sending notifications about alerts. Full access to rules for sending notifications about problems in program operation. |
| **Program settings: VIP status** | Read access. |
| **User rules: YARA** | Access only to export rules. |
| **Program settings: TAA exceptions** | Access to read and export. |
| **Program settings: Passwords to archives** | No access. |
| **Program 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 **Cluster management** 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 program web interface window, select the **Program settings section, Users** subsection. Click **Add**.

   This opens the **New user** window.
3. To enable an account, turn on the **State** 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.
4. In the **Role** drop-down list, select **Administrator**.
5. 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, digits 0–9, hyphens (-), and underscores (_).
   - Must begin with a letter (A–Z or a–z).
6. 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.

7. In the **Confirm password** field, re-enter the password that will be used to access the web interface.
8. 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 program web interface window, select the **Program settings section, Users** subsection. Click **Add**.

   This opens the **New user** window.
3. To enable an account, turn on the **State** 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.
4. In the **Role** drop-down list, select one of the following roles:
   - **Senior security officer**.
   - **Security officer**
5. 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, digits 0–9, hyphens (-), and underscores (_).
   - Must begin with a letter (A–Z or a–z).
6. 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.

7. In the **Confirm password** field, re-enter the user password that will be used to access the web interface.
8. 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.
9. 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 program web interface window, select the **Program settings** section, **Users** subsection. Select the account whose access rights you want to change.
   This opens the **Edit account** window.
3. If you want to enable or disable an account, move the **State** toggle switch.

4. 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 **Limited functionality** if you want to grant the user access only to the web interface of this PCN server.

5. 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.

6. Click **Save**.

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 program web interface window, select the **Program settings section**, **Users** subsection. In the list of accounts, select the user account that you want to enable or disable.
3. In the **State** 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.

4. 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 program web interface window, select the **Program settings section, Users** subsection. In the list of accounts, select the user account whose password you want to change.

   This opens the **Edit account** window.
3. 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.
4. In the **Confirm password** field, enter the new password again.
5. Click **Save**.

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 **Password change** action.

   This opens the **Password change** 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 **Password change**.

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 obtained from users around the globe. *Kaspersky Security Network* is designed to obtain such data.

Kaspersky Security Network (hereinafter also "KSN") is an infrastructure of online services that provides users with access to the Kaspersky 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 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 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 **Program settings** section, **KSN/KPSN and MDR** 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 **Apply**.

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 **Program settings** section, **KSN/KPSN and MDR** 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.xms, kh_private.xms and ksncli_private.dat files by using the **Browse** button.
5. Click **Apply**.

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 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 **Program 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.

   This opens the file selection window.
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.

   This opens the file selection window.
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 MD5 and SHA256 hashes of objects detected by the Sandbox component in 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 **Program settings** section, **KPSN reputation database** subsection.

3. Do one of the following:

   - Turn on the **Assign the "Untrusted" status to alerts** switch if you want the program to set the status of alerts to *Untrusted* and save information about Sandbox component alerts in the local reputation database of KPSN.
   - Turn off the **Assign the "Untrusted" status to alerts** switch if you do not want to save information about Sandbox component alerts in the local reputation database of KPSN.

4. Click **Save**.

The saving of information to the local reputation database of KPSN is configured.

# 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 **Program settings** section, **KSN/KPSN and MDR** subsection.
3. On the right of the **Connection type** parameter name, click the **Not connected** button.
4. Click **Apply**.

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.

   This opens the Sandbox component administrator credentials input window.

2. Enter the Sandbox component administrator user name and password that you specified when installing the Sandbox component.

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 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 **Start**.

# 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 update server**.

     The program connects to Kaspersky update server over HTTP and downloads up-to-date databases.

   - **Kaspersky secure update server**.

     The program connects to Kaspersky update server over HTTPS and downloads up-to-date databases. It is recommended to use HTTPS for database updates.

   - **Custom server**.

     The program connects to your FTP or HTTP server or to the folder with program databases on your computer to download up-to-date databases.

3. If you select **Custom server**, in the field under the name of the setting, enter the full path to the folder that contains the program database 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**.

   This opens the action selection window.
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**.

    This opens the action selection window.
12. Select the line containing the Sandbox server IP address.
13. Press **ENTER**.

    This opens the **Sandbox Key Fingerprint** window containing the Sandbox certificate thumbprint and a request to confirm the certificate thumbprint authenticity.
14. 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.
15. 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.

16. 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.

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 **Network 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 **Network 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.

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 **Network 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 **Network 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 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 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 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.

   This opens the file selection window.

3. Select an update file to download and click the **Open** button.

   This closes the file selection window.

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 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.

   This opens the file selection window.

3. Select an ISO file that you want to download and click the **Open** button.

   This closes the file selection window.

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.

   This opens the **Unpack** window. 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 **Save**.

# 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 **Settings** section in the Sandbox web interface window.
2. In the **System Log** settings group, click the **Download** button.
3. 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 Sandbox settings

*To export the Sandbox system parameters, proceed as follows:*

1. Select the **Settings** section in the Sandbox web interface window.
2. In the **Program 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 **Export**.

   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 Sandbox settings

*To import the Sandbox parameters, proceed as follows:*

1. Select the **Settings** section in the Sandbox web interface window.
2. In the **Program settings** settings group, click the **Import** button.

   This open 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 **Import**.

   This opens the file selection window.
4. Select a tar.gz file with the Sandbox parameters that you want to download and click the **Open** button.

   This closes the file selection window.

   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 **Settings** 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.

# Powering off the Sandbox server

*To shut down the Sandbox server, proceed as follows:*

1. Select the **Settings** 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 powers off.

# Changing the Sandbox administrator account password

*To change the Sandbox administrator account password, proceed as follows:*

1. Select the **Settings** section in the Sandbox web interface window.
2. The **Password change** settings group will show the Sandbox administrator account name that you set during installation of the Sandbox 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 **Password change**.

   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**.

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.
- **Cluster management**. Contains information about PCN and SCN servers about organizations in distributed solutions and multitenancy mode.
- **Endpoint Agents**. Contains information about computers with Kaspersky Endpoint Agent and their settings.
- **Program 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 display 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:

- **Processed**. Displays the processing state for traffic coming from Sensor component and Kaspersky Endpoint Agent program to the server with the Central Node component.
- **Queues**. Displays information on the number and volume of objects waiting to be scanned by the program modules and components.
- **Sandbox processing time**. 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.

## 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 right part of the program web interface window, 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 **Widgets**.
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 **Processed** widget, click + 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 **Save**.

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 **Save**.

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 **Download**.

   The layout in PDF format will be saved to the hard drive of your computer in the downloads folder of the browser.
6. Click **Close**.

# 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

In the **Processed** widget, you can assess the processing status of data coming from the Sensor component and Kaspersky Endpoint Agent program component to the server with the Central Node component, and track data drops.

To select the component (Sensor or Kaspersky Endpoint Agent) for which you want to assess incoming data, use the drop-down list to the right of the **Processed** widget name.

You can select the type of data display in the drop-down list to the right of the component name (Sensor or Kaspersky Endpoint Agent):

- **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 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 **Processed** widget has **(SPAN)** or **(ICAP)** Sensor type and **Current load** data display type selected and displays the data processing rate for SPAN and ICAP 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 Central Node component, indicated in green (Mbps).
- **Files**—Rate of file processing indicated in gray (objects per second).
- **URLs**—Rate of URL processing indicated in blue (objects per second).
- **Unprocessed**—Number of unprocessed objects 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.
  The **Processed** widget has **(SMTP)** Sensor type and **Current load** data display type selected and displays the data processing rate for mail traffic coming from the mail sensor 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 (messages per second).
- **Files**—Rate of file processing indicated in gray (objects per second).
- **URLs**—Rate of URL processing indicated in blue (objects per second).
- **Unprocessed**—Number of unprocessed objects 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.
  The **Processed** widget has **(LOAD) Endpoint Agents** Sensor type and **Current load** data display type selected and displays the processing rate for events coming from Endpoint Agent components to the server with the Central Node component over a specific time period (events per second).
  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 **Processed** widget with an **(SPAN)** or **(ICAP)** Sensor, **Selected period** data display type, and **Month** data display period selected, displaying the rate of SPAN and ICAP traffic coming to the server with the Central Node component, as well as the number of files and URLs extracted from mail traffic during 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 (objects per second).
- **Files**—Number of extracted files indicated in gray.
- **URLs**—Number of extracted URLs indicated in blue.
- **Unprocessed**—Number of unprocessed objects 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.
  The **Processed** widget with an **(SMTP)** Sensor, **Selected period** data display type, and **Month** data display period selected, displaying the data processing rate of mail traffic coming to the server with the Central Node component, as well as the number of files and URLs extracted from mail traffic during 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 (objects per second).
- **Files**—Number of extracted files indicated in gray.
- **URLs**—Number of extracted URLs indicated in blue.
- **Unprocessed**—Number of unprocessed objects 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.
  The **Processed** widget with **(LOAD) Endpoint Agents** Sensor type, **Selected period** data display type, and **Month** data display period selected, displaying the number of events coming from hosts with Kaspersky Endpoint Agent program to the server with the Central Node component during the selected month.
  When you move the mouse cursor over a widget, you will see a pop-up window that displays the number of events for 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 the amount of unprocessed data.

Data transfer in the queue is measured in messages.

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.
- **Unprocessed** – amount of unprocessed data 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 amount of unprocessed data 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 the working condition of modules and components of the program

If modules or components of the program encounter errors that the administrator is advised to look at, a yellow warning box is displayed in the upper part of the **Dashboard** section of the program web interface.

User with the **Local administrator** and **Administrator** role can access information about the working condition of 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 the working condition:

- If you are using a standalone Central Node server, the user can access information about the working condition of 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 information about the working condition of that SCN server for organizations whose data the user is allowed to access.
- If you are using the distributed solution and multitenancy mode, and the user is managing the PCN server, the user can access information about the working condition of the PCN server and all SCN servers connected to that server, for organizations whose data the user is allowed to access.

*For details about the working condition of program modules and components,*

click **View details** to open the **System health** window.

The **System health** window displays the following information:

- If program modules and components are operating normally, the OK icon is displayed in the corresponding row.
- If problems are detected that the administrator is advised to look at, an icon with the number of such problems (for example, 1) is displayed in the corresponding row.

  In this case, detailed problem information is displayed in the right part of the **System health** window.

The **System health** window contains the following sections:

- **Components health**—Performance status of program modules and components.

  Contains information on the operational status of program modules and components, the quarantine, and databases update on all servers where the program is operating.

  > Example:
  > 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.
  > To resolve the problem, make sure that update servers are available. If you are using a proxy server to connect to update servers, make sure the proxy server has no errors pertaining to the connection to Kaspersky Anti Targeted Attack Platform servers.

- **Processed**—State of receiving and processing incoming data. The status is generated based on the following criteria:
  - State of receiving data from servers with the Sensor component, from the server or virtual machine with the mail sensor, from Kaspersky Endpoint Agent hosts.
  - 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 Technical Support.

# 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.

- Generate or upload a server certificate that you can prepare on your own
- Configure the network settings of the server.

If you are using the distributed solution and multitenancy 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 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 **Program 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 **Apply**.

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 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 **Program 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.

# Generating or uploading a TLS certificate of the server

If you are already using a server TLS certificate, generating or uploading a new certificate causes the currently used certificate to be removed and replaced with the new certificate.

You must enter the data of the new certificate everywhere the old certificate was used.

If you replace the TLS certificate, you will need to

- Reauthorize mail sensors (KSMG, KLMS) on Central Node.
- Reconfigure connection of Central Node, PCN and SCN to Sandbox.

- Reconfigure Endpoint Agent traffic redirection to Sensor and trusted connection with Endpoint Agent.
- Upload a new certificate in Active Directory (if you use Active Directory).

Please delete all Endpoint Agent host isolation rules. Connection with the isolated hosts and control over them will be lost.

You can generate a new certificate in the web interface: of the Central Node server or upload a certificate that you have created independently.

If you are using the distributed solution and multitenancy mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

*To generate a TLS certificate for the Central Node server:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **General settings** subsection.
3. In the **TLS certificate** settings group, click the **Generate** button.

   This opens the action confirmation window.
4. Click **Yes**.

   Kaspersky Anti Targeted Attack Platform generates a new TLS certificate. The page is automatically refreshed.

   Communication with the mail sensors, the Sandbox component, and the Kaspersky Endpoint Agent program is interrupted until reauthorization.

You can choose to prepare the TLS certificate on your own and upload it using the Kaspersky Anti Targeted Attack Platform web interface.

The TLS certificate file prepared for upload 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 private key length must be 2048 bits or longer.

For more details on preparing TLS certificates for import, please refer to the documentation on Open SSL.

Upload the TLS certificate in the web interface of the PCN or SCN server to which you want to upload the certificate.

*To upload an independently prepared TLS certificate using the Kaspersky Anti Targeted Attack Platform web interface:*

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **General settings** subsection.
3. In the **TLS certificate** settings group, click the **Upload** button.

   This opens the file selection window.
4. Select a TLS certificate file to download and click the **Open** button.

   This closes the file selection window.

The TLS certificate is added to the Kaspersky Anti Targeted Attack Platform.

Communication with the mail sensors, the Sandbox component, and the Kaspersky Endpoint Agent program is interrupted until reauthorization.

# Downloading the TLS certificate of the server

If you are using the distributed solution and multitenancy mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

*To download the TLS certificate to your computer:*

1. In the Kaspersky Anti Targeted Attack Platform web interface window, select the **Program settings** section, **General settings** subsection.
2. In the **TLS certificate** 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 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 **Program 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 **Apply**.

The host name will be assigned.

# Configuring DNS settings

If you are using the distributed solution and multitenancy 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 **Program settings** section, **Network settings** subsection.
2. In the **DNS settings** settings group, in the **Domains** text box, enter the domain name.
3. In the **Primary and Secondary DNS servers** field, enter the IP addresses of DNS servers.
4. Click **Apply**.

The DNS settings will be configured.

# Configuring settings of the network interface

If you are using the distributed solution and multitenancy 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 **Program 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 **IP** field, specify the IP address of the network interface.
4. 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 **Save**.

The settings of the network interface will be configured.

# Configuring the default network route

If you are using the distributed solution and multitenancy 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 **Program 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 **Gateway** text box, enter the IP address of the gateway.
4. Click **Apply**.

The default network route will be configured.

# Configuring proxy server connection settings

If you are using the distributed solution and multitenancy 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 **Program 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 **Apply**.

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 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 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 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 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.

   This opens the Sensor component settings page.

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 **Apply**.

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 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.

   This opens the Sensor component settings page.

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 **Apply**.

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 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.

   This opens the Sensor component settings page.

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 **Apply**.

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 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.

   This opens the Sensor component settings page.

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.

      This opens the file selection window.

   b. Select the certificate file with the PEM extension and click the Open button.

9. Click **Apply**.

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 mode, use the web interface of the PCN or SCN server for which you want to configure parameters.

If you use a separate proxy server, by default, Kaspersky Anti Targeted Attack Platform does not encrypt ICAP traffic or authenticate ICAP clients. The application administrator must independently ensure a secure network connection between your proxy server and Kaspersky Anti Targeted Attack Platform by using traffic tunneling or iptables.

*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.

   This opens the Sensor component settings page.

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 **Apply**.

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 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.

   This opens the Sensor component settings page.

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 **Apply**.

Integration with the mail server via POP3 will be configured.

# Managing Kaspersky Endpoint Agent host information

Kaspersky Endpoint Agent 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 Kaspersky Endpoint Agent is installed, on the **Endpoint Agents** tab of the program web interface window for organizations whose data the user is allowed to access. If you are using distributed solution and multitenancy mode, the web interface of the PCN server displays the list of hosts with Kaspersky Endpoint Agent 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 Kaspersky Endpoint Agent installed, for organizations whose data they are allowed to access.

If suspicious network activity is detected, users with the **Senior security officer** role can isolate from the network any host with Kaspersky Endpoint Agent, for organizations whose data the user is allowed to access. In this case, the connection between the server with the Central Node component and a host with Kaspersky Endpoint Agent is not interrupted.

To provide support in case of problems with Kaspersky Endpoint Agent, Technical Support staff 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 obtained for debugging purposes. The extended diagnostic information that is obtained is saved on the user's computer. The retrieved data is not automatically sent to Kaspersky.

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 Agents section

If you are using multitenancy mode, prior to using the **Endpoint Agents** section you need to select the organization whose data you want to view.

*To select an organization for managing in the **Endpoint Agents** 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 Kaspersky Endpoint Agent host table on a standalone Central Node server

The table of Kaspersky Endpoint Agent hosts is located in the **Endpoint Agents** section of the program web interface window.

If you are using a standalone Central Node server, but not using distributed solution and multitenancy mode, the table of Kaspersky Endpoint Agent hosts can display the following data:

- Number of hosts and activity indicators of Kaspersky Endpoint Agent:
  - **Critical inactivity** is the number of hosts from which latest data was received a very long time ago.
  - **Warning** is the number hosts from which latest data was received a long time ago.
  - **Normal activity** is the number of hosts from which latest data was recently received.
- **Host**—Name of the host with Kaspersky Endpoint Agent.
- **IP**—IP address of the computer where Kaspersky Endpoint Agent is installed.
- **OS**—Version of the operating system that is installed on the computer with Kaspersky Endpoint Agent.
- **Version**—Version of Kaspersky Endpoint Agent installed.
- **Activity**—Activity indicator of Kaspersky Endpoint Agent. 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 a link in a 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 Kaspersky Endpoint Agent host table in distributed solution and multitenancy mode

The table of Kaspersky Endpoint Agent hosts is located in the **Endpoint Agents** section of the program web interface window.

If you are using the distributed solution and multitenancy mode, the table contains information about Kaspersky Endpoint Agent hosts connected to the PCN and all SCN servers. The table can display the following data:

- Number of hosts and activity indicators of Kaspersky Endpoint Agent:
  - **Critical inactivity** is the number of hosts from which latest data was received a very long time ago.
  - **Warning** is the number hosts from which latest data was received a long time ago.
  - **Normal activity** is the number of hosts from which latest data was recently received.
- **Host**—Name of the host with Kaspersky Endpoint Agent.
- **Servers**—Names of servers to which the Kaspersky Endpoint Agent host is connected.
- **IP**—IP address of the computer where Kaspersky Endpoint Agent is installed.
- **OS**—Version of the operating system that is installed on the host with Kaspersky Endpoint Agent.
- **Version**—Version of Kaspersky Endpoint Agent installed.
- **Activity**—Activity indicator of a host with Kaspersky Endpoint Agent. 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 a link in a 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 information about a host

*To view information about a host with Kaspersky Endpoint Agent:*

1. Select the **Endpoint Agents** 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:

- In the **Host** section:
  - **Name**—Name of the host with Kaspersky Endpoint Agent.
  - **IP**—IP address of the host where Kaspersky Endpoint Agent is installed.
  - **OS**—Version of the operating system on the host with the Kaspersky Endpoint Agent program installed.
  - **Server**—Name of the SCN or PCN server. Only displayed in distributed solution and multitenancy mode.
- In the **TLS certificate for Kaspersky Endpoint Agent connection** section:
  - **Endpoint Agent version**—Version of Kaspersky Endpoint Agent installed.
  - **Activity**—Activity indicator of Kaspersky Endpoint Agent. 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.
  - **Connected to server**—Name of the Central Node, SCN, or PCN server to which the host is connected.
  - **Last connection**—time of the last connection to the Central Node, SCN, or PCN server.
  - **License key status**—Information about the Kaspersky Endpoint Agent license key.

# Filtering and searching hosts with Kaspersky Endpoint Agent by host name

*To filter or search for hosts with the Kaspersky Endpoint Agent program by host name:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Host** link to open the filter configuration window.
3. If you want to display only isolated hosts, select the **Show isolated Endpoint Agents only** check box.
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 host name.
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 **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

## Filtering and searching hosts with Kaspersky Endpoint Agent that have been isolated from the network

*To filter or search for hosts with the Kaspersky Endpoint Agent program that are isolated from the network:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Host** link to open the filter configuration window.
3. Select the **Show isolated Endpoint Agents only** check box.
4. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

## Filtering and searching hosts with Kaspersky Endpoint Agent by PCN and SCN server names

If you are using distributed solution and multitenancy mode, you can filter or find hosts with the Kaspersky Endpoint Agent program based on the names of PCN and SCN servers to which those hosts are connected.

*To filter or search for hosts with the Kaspersky Endpoint Agent program by the names of PCN and SCN servers:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
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 Kaspersky Endpoint Agent program.

4. Click **Apply**.

The filter configuration window closes.

The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by computer IP address

*To filter or search for hosts with the Kaspersky Endpoint Agent program based on the IP address of the computer with the Kaspersky Endpoint Agent program installed:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

2. Click the **IP** link to open the filter configuration window.

3. In the drop-down list, select one of the following filtering operators:

   - **Contains**.
   - **Does not contain**.

4. 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`).

5. To add a filter condition using a different criterion, click + and specify the filter condition.

6. If you want to delete the filter condition, click the button to the right of the field.

7. Click **Apply**.

The filter configuration window closes.

The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by operating system version on the computer

*To filter or search for hosts with the Kaspersky Endpoint Agent program based on the version of the operating system installed on the computer hosting the Kaspersky Endpoint Agent program:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **OS** link to open the filter configuration window.
3. In the drop-down list, select one of the following filtering operators:
   - **Contains**.
   - **Does not contain**.
4. In the entry field, specify one or several characters of the operating system version.
5. To add a filter condition using a different criterion, click + and specify the filter condition.
6. If you want to delete the filter condition, click the button to the right of the field.
7. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by Kaspersky Endpoint Agent version

*To filter or search for hosts with the Kaspersky Endpoint Agent program based on the version of the Kaspersky Endpoint Agent program:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Version** link to open the filter configuration window.

3. In the drop-down list, select one of the following filtering operators:

   - **Contains**.
   - **Does not contain**.

4. In the entry field, specify one or several characters of the version of the Kaspersky Endpoint Agent program.

5. To add a filter condition using a different criterion, click + and specify the filter condition.

6. If you want to delete the filter condition, click the button to the right of the field.

7. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent based on their activity

*To filter or search for hosts with the Kaspersky Endpoint Agent program by their activity:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.

2. Click the **Activity** link to open the filter configuration window.

3. Select the check boxes next to one or more Kaspersky Endpoint Agent program activity indicators:

   - **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.

4. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Quickly creating a filter for hosts with Kaspersky Endpoint Agent

*To quickly create a filter for hosts with the Kaspersky Endpoint Agent program:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

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 displays only those hosts that match the filter criteria you have set.

# Resetting the hosts with Kaspersky Endpoint Agent filter

*To clear a filter for hosts with Kaspersky Endpoint Agent program based on one or multiple filter conditions:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
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 displays only those hosts that match the filter criteria you have set.

# Configuring activity indicators of Kaspersky Endpoint Agent

Users with the **Local administrator** and **Administrator** permissions can define what durations of inactivity of computers with Kaspersky Endpoint Agent correspond to normal, low, or very low activity, and can configure the activity indicators for Kaspersky Endpoint Agent program. All users can view Kaspersky Endpoint Agent indicators.

*To configure activity indicators for Kaspersky Endpoint Agent program:*

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 **Program settings** section, **Endpoint Agents** subsection.
3. In the fields under the section name, enter the number of days of inactivity of computers with Kaspersky Endpoint Agent that you want to display as **Warning** and **Critical inactivity**.
4. Click **Apply**.

Users with **Senior security officer** and **Security officer** permissions can see activity indicators that you configured for Kaspersky Endpoint Agent in the **Activity** field of the Kaspersky Endpoint Agent host table in the **Endpoint Agents** section of the program web interface.

# Supported interpreters and processes

Kaspersky Endpoint Agent program monitors the execution of scripts by the following interpreters:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msiexec.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 Kaspersky Endpoint Agent program is presented in the table below.

Processes and the file extensions that they open

| Process | File extensions |
|---|---|
| winword.exe | rtf<br>doc<br>dot<br>docm<br>docx<br>dotx<br>dotm<br>docb |
| excel.exe | xls<br>xlt<br>xlm<br>xlsx<br>xlsm<br>xltx<br>xltm<br>xlsb<br>xla<br>xlam<br>xll<br>xlw |

| Process | File extensions |
| --- | --- |
| powerpnt.exe | ppt<br>pot<br>pps<br>pptx<br>pptm<br>potx<br>potm<br>ppam<br>ppsx<br>ppsm<br>sldx<br>sldm |
| acrord32.exe | pdf |
| wordpad.exe | docx<br>pdf |
| chrome.exe | pdf |
| MicrosoftEdge.exe | pdf |

# 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:

1. **Creating a request to connect to the Sandbox component**

   You can create a request in the administrator menu or in the program web interface 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.

2. **Processing a connection request 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.
- **State**—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.

   This opens the **Sandbox connection** window.
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 **State** 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 **Limited functionality**.

3. Click **Apply**.

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.

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:

1. **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 or the Kaspersky Security for Linux Mail Server Help Guide.

   To integrate other external systems, use the REST API.

2. **Confirm integration for Kaspersky Anti Targeted Attack Platform**

   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.

3. **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 Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (hereinafter also "MDR") detects and prevents fraud in the client's infrastructure. MDR provides continuous managed protection and allows organizations to automatically discover hard-to-detect threats while freeing up IT security personnel to work on issues requiring their participation.

Kaspersky Anti Targeted Attack Platform obtains data and sends it to Kaspersky Managed Detection and Response using a Kaspersky Security Network stream. Therefore, participation in KSN is necessary for configuring integration with MDR.

Integration with MDR is only available if at least one KATA or EDR license is active. If only one license key (only KATA or only EDR) is added in the program, statistics is limited to the functionality provided by that license. If both license keys are added in the program, complete statistics is sent.

Before configuring the integration of Kaspersky Anti Targeted Attack Platform with the MDR program, you must download an archive with the configuration file from the MDR portal.

Only Local Administrator and Web Interface Administrator can configure the integration with MDR.

# Enabling the MDR integration

Make sure that an active license key is added and participation in KSN is configured in the program. Otherwise the MDR integration is unavailable.

*To enable the MDR integration:*

1. Log in to the program web interface with the administrator account.
2. Select the **Program settings** section, **KSN/KPSN and MDR** subsection.
3. Under **MDR Integration**, click **Upload** to upload the configuration file.

   This opens the file selection window.
4. Select the archive you downloaded during registration at the MDR portal and click **Open**.

   The following information about the MDR license is displayed in the window:

   - **Serial number**.
   - **Expiration date**.
   - **Days remaining**.

Integration with MDR is enabled. Integration settings configured in the configuration file are applied to all connected Sensor components. MDR starts using alert statistics sent via the KSN stream.

# Disabling the MDR integration

*To disable the MDR integration:*

1. Log in to the program web interface with the administrator account.
2. Select the **Program settings** section, **KSN/KPSN and MDR** subsection.
3. Under **MDR Integration**, click **Delete file**.
4. In the confirmation window, click **Yes**.

The configuration file is deleted and the MDR integration is disabled. Statistics is still sent to KSN servers but this information is not used by MDR.

## Replacing the MDR configuration file

*To replace the MDR configuration file:*

1. Log in to the program web interface with the administrator account.
2. Select the **Program settings** section, **KSN/KPSN and MDR** subsection.
3. Under **MDR Integration**, click **Replace file**.

   This opens the file selection window.
4. Select a new archive containing a configuration file and click **Open**.

   MDR license information is updated in the program web interface.

The configuration file is replaced. New integration settings are applied to all connected Sensor components.

# 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 **Program 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 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 **Program 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 **Program 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.
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 **Program 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.

# Uploading 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 **Program 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.

   This opens the file selection window.
4. Select a TLS certificate file to download and click the **Open** button.

   This closes the file selection window.

   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: 3.7.0-1077.

- 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`<br>A file was detected in network traffic. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `dst` = <destination IP address>.<br>• `dpt` = <destination port>.<br>• `src` = <source IP address>.<br>• `spt` = <source port>.<br>• `shost` = <name of the host on which the file was detected>.<br>• `suser` = <user name>.<br>• `fName` = <name of the file within the compound object>.<br>• `fsize` = <size of the file within the compound object (in bytes)>.<br>• `fileType` = <format of the file within the compound object>.<br>• `fileHash` = <MD5 hash of the file within the compound object>.<br>• `KasperskyLabKATAcompositeFilePath` = <name of the compound object>.<br>• `KasperskyLabKATAcompositeFileSize` = <total size of the compound object (in bytes)>.<br>• `KasperskyLabKATAcompositeFileHash` = <MD5 hash of the compound object>.<br>• `KasperskyLabKATAfileSHA256` = <SHA256 hash of the compound object>.<br>• `cs2` = <technology that was used to detect the file>.<br>• `cs3Label` = <name of the virtual machine on which the file was detected> (only for the Sandbox component).<br>• `cs1` = <list of types of the detected objects according to the Kaspersky Lab classification>.<br>• `cs3` = <version of databases used to scan the file>.<br>• `app` = <name of the application-level protocol> (HTTP(S) or FTP).<br>• `requestMethod` = <HTTP request method> (only for the HTTP(S) protocol).<br>• `requestClientApplication` = <User Agent of the client computer> (only for the HTTP(S) protocol).<br>• `request` = <URL of the detected object> (only for the HTTP(S) protocol).<br>• `requestContext` = <HTTP Referer header> (only for the HTTP(S) protocol). |
| `file_mail` | `File from mail detected`<br>A file was detected in mail traffic. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `fName` = <name of the file within the compound object>.<br>• `fsize` = <size of the file within the compound object (in bytes)>.<br>• `fileType` = <format of the file within the compound object>.<br>• `fileHash` = <MD5 hash of the file within the compound object>.<br>• `KasperskyLabKATAcompositeFilePath` = <name of the compound object>.<br>• `KasperskyLabKATAcompositeFileSize` = <total size of the compound object (in bytes)>.<br>• `KasperskyLabKATAcompositeFileHash` = <MD5 hash of the compound object>.<br>• `KasperskyLabKATAfileSHA256` = <SHA256 hash of the compound object>.<br>• `cs2` = <technology that was used to detect the file>.<br>• `cs3Label` = <name of the virtual machine on which the file was detected> (only for the Sandbox component).<br>• `cs1` = <list of types of the detected objects according to the Kaspersky Lab classification>.<br>• `cs3` = <version of databases used to scan the file>.<br>• `externalId` = <Email message ID>.<br>• `suser` = <email address of sender>.<br>• `duser` = <email addresses of recipients>.<br>• `msg` = <message subject>. |
| `ids` | `IDS event detected`<br>An alert was generated by the Intrusion Detection System module. | • `eventId` = <alert ID>.<br>• `requestMethod` = <HTTP request method> (only for the HTTP(S) protocol).<br>• `requestClientApplication` = <User Agent of the client computer> (only for the HTTP(S) protocol).<br>• `rt` = <date and time of alert>.<br>• `dst` = <destination IP address>.<br>• `dpt` = <destination port>.<br>• `src` = <source IP address>.<br>• `spt` = <source port>.<br>• `proto` = <name of the network-level protocol> (TCP or UDP).<br>• `cs1` = <type of the detected object according to the Kaspersky Lab classification>.<br>• `cs2Label` = <name of the IDS rule>.<br>• `cs2` = <number of the IDS rule>.<br>• `cs3` = <Intrusion Detection System module database version>.<br>• `requestMethod` = <HTTP request method> (only for the HTTP protocol). |

| Alert type | Alert name and description | Key and description of its value |
| --- | --- | --- |
| | | • `requestClientApplication` = <User Agent of the client computer> (only for the HTTP protocol).<br>• `request` = <URL of the detected object>. |
| `url_web` | `URL from web detected`<br>An alert was generated by URL Reputation technology or Sandbox in network traffic. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `dst` = <destination IP address>.<br>• `dpt` = <destination port>.<br>• `src` = <source IP address>.<br>• `spt` = <source port>.<br>• `shost` = <name of the host on which the file was detected>.<br>• `suser` = <user name>.<br>• `cs1` = <list of categories to which the URL of the detected object belongs>.<br>• `requestMethod` = <HTTP request method>.<br>• `requestClientApplication` = <User Agent of the client computer>.<br>• `request` = <URL of the detected object>.<br>• `requestContext` = <HTTP Referer header>.<br>• `reason` = <HTTP response code>. |
| `url_mail` | `URL from mail detected`<br>An alert was generated by URL Reputation technology or Sandbox in mail traffic. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `externalId` = <Email message ID>.<br>• `suser` = <email address of sender>.<br>• `duser` = <email addresses of recipients>.<br>• `msg` = <message subject>.<br>• `request` = <URL of the detected object>.<br>• `cs2` = <technology that was used to generate the alert> (Sandbox or URL Reputation).<br>• `cs3Label` = <name of the virtual machine on which the file was detected> (only for Sandbox).<br>• `cs1` = <list of types of the detected objects according to the Kaspersky Lab classification> (for the Sandbox component) or <list of categories> (for URL Reputation).<br>• `cs3` = <version of databases used to scan the file> (only for Sandbox). |
| `dns` | `DNS request detected`<br>An alert was generated by URL Reputation technology in DNS traffic. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `dst` = <destination IP address>.<br>• `dpt` = <destination port>.<br>• `src` = <source IP address>.<br>• `spt` = <source port>.<br>• `shost` = <name of the host on which the file was detected>.<br>• `suser` = <user name>.<br>• `cs2` = <list of URL categories to which the domain names belong>.<br>• `requestMethod` = <type of DNS message> (request or response).<br>• `flexString1` = <type of record from the DNS request>.<br>• `dhost` = <host name from the DNS request>.<br>• `cs1` = <list of domain names from the DNS response>. |
| `file_endpoint` | `File from endpoint detected`<br>An alert was generated by the Endpoint Sensors component on the user's computer and contains a file. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `src` = <source IP address>.<br>• `shost` = <name of the host on which the file was detected>.<br>• `fName` = <name of the file within the compound object>.<br>• `fsize` = <size of the file within the compound object (in bytes)>.<br>• `fileType` = <format of the file within the compound object>.<br>• `fileHash` = <MD5 hash of the file within the compound object>.<br>• `KasperskyLabKATAcompositeFilePath` = <name of the compound object>.<br>• `KasperskyLabKATAcompositeFileSize` = <total size of the compound object (in bytes)>.<br>• `KasperskyLabKATAcompositeFileHash` = <MD5 hash of the compound object>.<br>• `KasperskyLabKATAfileSHA256` = <SHA256 hash of the compound object>.<br>• `cs2` = <technology that was used to detect the file>.<br>• `cs3Label` = <name of the virtual machine on which the file was detected> (only for the Sandbox component).<br>• `cs1` = <list of types of the detected objects according to the Kaspersky Lab classification>.<br>• `cs3` = <version of databases used to scan the file>.<br>• `app` = <name of the application-level protocol> (HTTP(S) or FTP).<br>• `FilePath` = <path to the file on the computer with the Endpoint Sensors component>. |
| `iocScanning` | `IOC has tripped on endpoint` | • `eventId` = <alert ID>. |

| Alert type | Alert name and description | Key and description of its value |
|---|---|---|
| | The alert was generated as a result of an IOC scan of computers with the Endpoint Sensors component.<br>This type of alert is available if you are using only KEDR functionality. | • `rt` = <date and time of alert>.<br>• `src` = <source IP address>.<br>• `shost` = <name of the host on which the file was detected>.<br>• `cs1` = <name of the IOC file by which the alert was generated>. |
| `taaScanning` | `TAA has tripped on events database`<br>Alert resulting from the TAA analysis of events.<br>This type of alert is available if you are using only KEDR functionality. | • `eventId` = <alert ID>.<br>• `rt` = <date and time of alert>.<br>• `shost` = <name of the host on which the alert was generated>.<br>• `cs1` = <name of the TAA rule by which the alert was generated>. |
| `heartbeat` | Periodic message containing the state of components. | • `dvc` = <IP address of the server with the Central Node component>.<br>• `rt` = <event date and time>.<br>• `KasperskyLabKATAcomponentName` = <name of the component>.<br>• `KasperskyLabKATAcomponentState` = <status of the component> (`0` – OK, `>0` – Error). |

# 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 **Program 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 **Apply**.

The settings of the server used for sending notifications will be configured.

# Database Update

*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 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 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 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 **Program 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 update server**.

     The program connects to Kaspersky update server over HTTP and downloads up-to-date databases.
   - **Kaspersky secure update server**.

     The program connects to Kaspersky update server over HTTPS and downloads up-to-date databases. It is recommended to use HTTPS for database updates.
   - **Custom server**.

     The program connects to your FTP or HTTP server or to the folder with program databases on your computer to download up-to-date databases.
3. If you have selected **Custom server**, in the field under the name of this setting, enter the URL of the update package on your HTTP server or the full path to the folder on your computer containing the application database update package.
4. Click **Apply**.

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 **Program 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 **Program 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 **Apply**.

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**.

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.
- **User rules**: **TAA**, **IDS**, **IOC**, and **YARA**. Contains information for managing user-defined rules.
- **Storage**: **Files**, and **Quarantine** Contains information for managing objects in quarantine and Storage.
- **Endpoint Agents**. Contains information about managing the Kaspersky Endpoint Agent program and viewing data.

- **Reports**: **Generated Reports** and **Templates**. Contains a report builder and a list of generated reports about alerts.

- **Program settings**: **IOC scanning schedule**, **Endpoint Agents**, **KPSN reputation database**, **Notifications**, **VIP status**, **White lists**, **Passwords to archives**, and **License**. 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, the white list and IDS and TAA (IOA) rules excluded from scanning, 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 working in 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 display 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.

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 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.
  - **Alerts by attack vector**. Displays detected objects based on the vector of the attack.
  - **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 experience.
  - **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 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.

  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:
  - **Domains**. 10 domains most frequently seen in alerts.
  - **IP addresses**. 10 IP addresses most frequently seen in alerts.
  - **Email senders**. 10 email senders most frequently seen in alerts.
  - **Email recipients**. 10 email recipients most frequently seen in alerts.
  - **TAA hosts**. 10 hosts that occur most frequently in events and alerts generated by the Targeted Attack Analyzer (TAA) technology.
  - **TAA rules**. 10 TAA (IOA) rules that occur most frequently in events and alerts generated by the Targeted Attack Analyzer (TAA) technology.

  The left part of each widget lists the domains, addresses of recipients, IP addresses, and addresses of message senders, host names, and TAA (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.

  By clicking the link with the name of each domain, recipient address, IP address, message sender address, host name, and TAA (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 **Widgets**.
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 **Save**.

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 **Save**.

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 **Download**.

   The layout in PDF format will be saved to the hard drive of your computer in the downloads folder of the browser.
6. Click **Close**.

# 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 scale

You can configure the display scale for "Alerts" widgets. You can configure the display scale of a widget if it has the icon in the upper right corner.

*To configure the display scale 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 scale of the selected widget is changed.

6. Repeat the steps for all widgets whose display scale you want to change.

7. Click **Save**.

The display scale of widgets is configured.

# Main principles of working with "Alerts" widgets

You can configure the display scale 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 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.

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.
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 and select the organization 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.

# Viewing the working condition of modules and components of the program

If modules or components of the program encounter errors that the administrator is advised to look at, a yellow warning box is displayed in the upper part of the **Dashboard** section of the program web interface.

User with the **Local administrator** and **Administrator** role can access information about the working condition of 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 the working condition:

- If you are using a standalone Central Node server, the user can access information about the working condition of 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 information about the working condition of that SCN server for organizations whose data the user is allowed to access.
- If you are using the distributed solution and multitenancy mode, and the user is managing the PCN server, the user can access information about the working condition of the PCN server and all SCN servers connected to that server, for organizations whose data the user is allowed to access.

*For details about the working condition of program modules and components,*

click **View details** to open the **System health** window.

The **System health** window displays the following information:

- If program modules and components are operating normally, the OK icon is displayed in the corresponding row.
- If problems are detected that the administrator is advised to look at, an icon with the number of such problems (for example, 1) is displayed in the corresponding row.

  In this case, detailed problem information is displayed in the right part of the **System health** window.

The **System health** window contains the following sections:

- **Components health**—Performance status of program modules and components.

  Contains information on the operational status of program modules and components, the quarantine, and databases update on all servers where the program is operating.

  Example:
  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.
  To resolve the problem, make sure that update servers are available. If you are using a proxy server to connect to update servers, make sure the proxy server has no errors pertaining to the connection to Kaspersky Anti Targeted Attack Platform servers.

- **Processed**—State of receiving and processing incoming data. The status is generated based on the following criteria:
  - State of receiving data from servers with the Sensor component, from the server or virtual machine with the mail sensor, from Kaspersky Endpoint Agent hosts.
  - 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 Technical Support.

# 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.
  - Google.
  - Apple.
  - Microsoft.

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.

You can sort alerts in the table by **Created** or **Updated**, **Importance**, **Update source**, and **State** columns.

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 security or corporate LAN security based on Kaspersky 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. **Update 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. 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**.
- **(IOC) IOC**.

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 KL TIP**.
  - **Create a prevention rule**.
  - **Copy value to clipboard**.
- SHA256 hash:
  - **Filter by this value**.
  - **Exclude from filter**.
  - **Find events**.
  - **Find on KL TIP**.
  - **Create a prevention rule**.
  - **Copy value to clipboard**.

- Destination IP address: **Find events**.
- Alert state:
  - **Assign to me**.
  - **Mark as processed**.

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, sorting, 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.

You can also sort alerts in the table by **Created** or **Updated**, **Importance**, **Update source**, and **State** columns.

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.

   This opens the table of alerts.

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 sell 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.

   This opens the table of alerts.

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 **Apply**.

   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 experience.

*To filter alerts based on their importance level:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

2. Click to expand the filter settings list.

3. Select one or several of the following alert importance levels:

   - **Low**—Alert has a low level of importance.
   - **Medium**—Alert has a medium level of importance.
   - **High**—Alert has a high level of importance.

   If no value is selected, the table shows alerts of all importance levels.

4. Click **Apply**.

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.

   This opens the table of alerts.

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 **Apply**.

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.

   This opens the table of alerts.
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 **Apply**.

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 **Update 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.
   This opens the table of alerts.
2. Click the **Update 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 **Apply**.

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.
   This opens the table of alerts.
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 **Apply**.

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. 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.
   This opens the table of alerts.
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 **Apply**.

The table of alerts displays only alerts matching the filter criteria you have set.

# Filtering and searching alerts by technology name

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 by technology name:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

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 to the right of the alert filtering operator that you have selected, select the name of the technology 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**.
   - **(IOC) IOC**.

   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 **Apply**.

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.

   This opens the table of alerts.

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 **Apply**.

The table of alerts displays only alerts matching the filter criteria you have set.

# Sorting alerts in the table

You can sort alerts in the table by **Created** or **Updated**, **Importance**, **Update source**, and **State** columns.

*To sort the alerts in the alert table:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

2. If you want to sort the alerts by date, click one of the icons to the right of the **Created** (if the table is displaying alert creation dates) or **Updated** (if the table is displaying alert update dates) column header:

   - ↑ to display newer alerts at the top of the table.
   - ↓ to display older alerts at the top of the table.

3. If you want to sort the alerts by the level of importance, to the right of the icon, click one of the following icons:

   - to display high importance alerts at the top of the table.
   - to display low importance alerts at the top of the table.

4. If you want to sort alerts by the address of the source of the detected object, click one of the icons to the right of the **Update source** column header:

   - to sort alphabetically, A–Z.
   - to sort alphabetically, Z–A.

5. If you want to sort alerts by the state of processing by the user, click one of the icons to the right of the **State** column header:

   - to sort alerts by state in the order of processing: **New** – **Rescan** – **In process** – **Processed**.
   - to sort alerts by state in the reverse order of processing: **Processed** – **In process** – **Rescan** – **New**.

# Quickly creating an alert filter

*To quickly create an alert filter:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

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.

   This opens the table of alerts.

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 Kaspersky Endpoint Agent (previously known as Endpoint Sensors) installed on 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 web traffic scanning for signs of intrusion into the corporate IT infrastructure according to preset rules, performed by the Intrusion Detection System module (IDS).
- Results of network activity scanning performed using Kaspersky TAA (IOA) rules.
- Results of network activity scanning performed using TAA (IOA), IDS, IOC user rules.

If the program detects processes running on a corporate LAN computer where the Kaspersky Endpoint Agent program is installed, the program web interface can display the following information:

- General information about the alert and processes running on the computer.
- Results of network activity scanning performed for the computer using Kaspersky TAA (IOA) rules.
- Results of network activity scanning performed for the computer using TAA (IOA), IOC user rules.

# Viewing alert details

*To view information about an alert:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

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 of any type

Regardless of the technology that was used to create the 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.

The upper part of the window containing alert information may display the following general information about the alert:

- **State**—Alert status depending on whether or not this alert has been processed by the user of Kaspersky Anti Targeted Attack Platform.
- **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 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.
- **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:

- File name.

  To expand the **Copy value to clipboard** action, click the link with the file name.

- File type. For example: ExecutableWin32.

  The **Find on KL TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

  Click **Create a prevention rule** to prevent the file from running.

  Click **Download file** to download the file to your computer's hard drive.

  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.

- File size in kilobytes.

- **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 KL TIP**.
  - **Find events**.

- **Find alerts**.
- **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 KL TIP**.
  - **Find on virustotal.com**.
  - **Find events**.
  - **Find alerts**.
  - **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.

# 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 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, Post, or Connect.
- **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 KL TIP by URL**.
  - **Find on KL TIP by domain name**.

- **Find events**.
- **Find alerts**.
- **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 KL TIP**.
  - **Find events**.
  - **Find alerts**.
  - **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:

  - **YARA**—Category of the detected file in YARA rules (for example, the category name susp_fake_Microsoft_signer can be displayed).

    The **Find on KL TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

    Click **Create a prevention rule** to prevent the file from running.
  - **SB** (Sandbox)—Results of the file behavior analysis performed by the Sandbox component.

    You can click **Sandbox detect** to open a window with detailed information about the results of file behavior analysis.

    The **Find on KL TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

    Click **Create a prevention rule** to prevent the file from running.

    You can download a detailed log of file behavior analysis in all operating systems by clicking **Download debug info**.

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.

- **URL** (URL Reputation) is the category of a malicious, phishing URL or an URL that has been previously used by attackers for targeted attacks on corporate IT infrastructures.

- **IDS** (Intrusion Detection System) is the category of the detected object based on the Intrusion Detection System database or the name of the IDS user rule that was used to create the alert. For example, the displayed category can be Trojan-Clicker.Win32.Cycler.a.

  Click the link to display the category of the object in the Kaspersky Threats database.

- **AM** (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.

  Click the link to display the category of the object in the Kaspersky Threats database.

  The **Find on KL TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

  Click **Create a prevention rule** to prevent the file from running.

  Click **Download file** to download the file to your computer's hard drive.

- **TAA** (Targeted Attack Analyzer)—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

  Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.

- **IOC**—Name of the IOC file used to create the alert.

  Select an IOC file to open a window with the results of the IOC scan.

  Click **Find events** to display the **Threat Hunting** event table in a new browser tab. A search filter is configured in the search criteria, for example, by **MD5**, **FileFullName**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

# Information in the IDS rule section

The **IDS rule** section displays information about the alert made by the IDS (Intrusion Detection System) technology as a hex-editor matrix.

The *hex-editor* or hexadecimal editor is an application for editing data where data is represented as a sequence of bytes.

The upper part of the matrix displays the length of the IDS rule.

The left part of the matrix displays the data of the rule in text format.

The **Rule details** subsection of the **IDS rule** section displays the header of the IDS rule and data of the IDS alert in the Suricata format. For example, it can display information about the direction of the traffic (`flow`), the HTTP request method (`http_method`), the HTTP header (`http_header`), the security ID (`sid`).

# Information in the Network event section

The **Network event** section can show the following information about the link to the website opened on the computer:

- **Date** and **Time**—Date and time of the network event.
- **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**—IP address of the computer on which the website link was opened.
- **URL**—Type of the HTTP request, for example, GET or POST, and the URL of the website.

  Clicking the link with the URL opens a list in which you can select one of the following actions:

  - **Find on KL TIP by URL**.
  - **Find on KL TIP by domain name**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.
- **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.

# Scan results in Sandbox

The object scan results window in Sandbox can display the following alert details:

- **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 KL TIP**.
  - **Find events**.
  - **Find alerts**.

- **Create a prevention rule**.
- **Copy value to clipboard**.

- **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.

You can click **New prevention rule** in the upper right corner of the window to prevent the file from running.

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 links in the **Destination IP** column opens a list in which you can select one of the following actions:
  - **Find on KL TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

  Clicking links in the **URL** column opens a list in which you can select one of the following actions:
  - **Find on KL TIP by URL**.
  - **Find on KL TIP by domain name**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

- **IDS activity log**—Log of the file's network activity. 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.

  Clicking links in the **Destination IP** column opens a list in which you can select one of the following actions:
  - **Find on KL TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

  Clicking links in the **URL** column opens a list in which you can select one of the following actions:
  - **Find on KL TIP by URL**.
  - **Find on KL TIP by domain name**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.
- **DNS activity log**—Log of the file's DNS activity. It contains the following information:
  - Request type (Request or Response)
  - **DNS Name** —Domain name of the server.
  - **Type** —Type of DNS request, for example A or CNAME.
  - **Host**—Host name or IP address that was interacted with.

  Clicking the links in the **DNS Name** or **Host** columns opens a list in which you can select one of the following actions:
  - **Find on KL TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

You can click **Download full log** in the lower part of each scanning mode (**Quick scan mode** and **Full logging mode**) to download the log of file behavior analysis in each operating system to your computer

# IOC scan results

The IOC alert processing result window displays the following information:

- In the **File** section:
  - **File size**.
  - **Full path**. Clicking the link with **Full path** opens a list in which you can select one of the following actions:
    - Find events.
    - Find alerts.
    - Run the following tasks:
      - Kill process.
      - Delete file.
      - Get file.
      - Quarantine file.
    - **Copy value to clipboard**.
- **SHA256**. Clicking the **SHA256** link opens a list in which you can select one of the following actions:
  - **Find on KL TIP**.
  - **Find on virustotal.com**.
  - **Find events**.
  - **Find alerts**.
  - **Create a prevention rule**.
  - **Copy value to clipboard**.
- **MD5**. Clicking the **MD5** link opens a list in which you can select one of the following actions:
  - Find on KL TIP.
  - Find events.
  - Find alerts.

- Create a prevention rule.
- **Copy value to clipboard**.

- The **IOC** section provides the XML code of the IOC file. The criterion by which the alert was generated is highlighted in yellow.

## Information in the Hosts section

The **Hosts** section displays the following information about hosts on which the TAA (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 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 rule.

## 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 with data about an alert (except the URL Reputation and IOC technologies) for further analysis.

To do so, you must copy the alert data to the clipboard and then email it to Kaspersky.

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 for further analysis.

*To copy alert data to the clipboard:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

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** link in the lower part of the window containing alert information.

   This opens the **Details** window.

4. View the alert data to be sent to Kaspersky.

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 for further analysis.

# Recommendations for processing alerts

Information about alerts made by AM (Anti-Malware Engine), SB (Sandbox), YARA, IOC, and IDS (intrusion Detection System) technologies that is displayed in the right part of the window includes recommendations on processing these alerts.

*To view information about an alert:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

2. Click the line containing the alert whose information you want to view.

This opens a window containing information about the alert.

# Recommendations for processing AM alerts

In the right part of the window, the **Recommendations** section displays recommendations that you can follow, as well as the number of alerts or events that have attributes in common with the alert you are working on.

*You can follow the following recommendations:*

- Under **Qualifying**, expand the **Find related alerts** list.

  A list of attributes is displayed that can be used to find similar alerts, and the number of similar alerts for each attribute.

Select one of the following attributes:

- **By MD5**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the MD5 hash. The MD5 hash of the file from the alert you are working on is highlighted in yellow.
- **By SHA256**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the SHA256 hash. The SHA256 hash of the file from the alert you are working on is highlighted in yellow.
- **By host name**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The host name from the alert you are working on is highlighted in yellow.
- **By sender address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The sender address of the email message from the alert you are working on is highlighted in yellow.
- **By recipient address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Destination** column. The recipient address of the email message from the alert you are working on is highlighted in yellow.
- **By URL**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the URL from the alert you are working on.

- Under **Qualifying**, select **Find related KES events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the **Detect processing result** event type is selected and a search filter is configured, for example, by **RemoteIP**, **MD5**, **SHA256**, **URI**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

  The action is only available if you are using KEDR functionality and a KEDR license key has been added.

- Under **Investigation**, select **Find related events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, a search filter is configured, for example, by **RemoteIP**, **MD5**, **SHA256**, **URI**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

  The action is only available if you are using KEDR functionality and a KEDR license key has been added.

# Recommendations for processing SB alerts

In the right part of the window, the **Recommendations** section displays recommendations that you can follow, as well as the number of alerts or events that have attributes in common with the alert you are working on.

*You can follow the following recommendations:*

- Under **Qualifying**, expand the **Find related alerts** list.

  A list of attributes is displayed that can be used to find similar alerts, and the number of similar alerts for each attribute.

Select one of the following attributes:

- **By MD5**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the MD5 hash. The MD5 hash of the file from the alert you are working on is highlighted in yellow.
- **By SHA256**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the SHA256 hash. The SHA256 hash of the file from the alert you are working on is highlighted in yellow.
- **By host name**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The host name from the alert you are working on is highlighted in yellow.
- **By sender address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The sender address of the email message from the alert you are working on is highlighted in yellow.
- **By recipient address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Destination** column. The recipient address of the email message from the alert you are working on is highlighted in yellow.
- **By URL**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the URL from the alert you are working on.
- **By URL from Sandbox**. Click the link to display the **Alerts** table in a new browser tab. The alerts are filtered by the **Details** column, that is, the URL address from the alert you are working on, as well as all URLs that were found to be relevant by the Sandbox component as the alert was processed.

- Under **Qualifying**, select **Find related KES events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the **Detect processing result** event type is selected and a search filter is configured, for example, by **RemoteIP**, **MD5**, **SHA256**, **URI**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

  The action is only available if you are using KEDR functionality and a KEDR license key has been added.

- Under **Investigation**, select **Find related events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, a search filter is configured, for example, by **RemoteIP**, **MD5**, **SHA256**, **URI**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

  The action is only available if you are using KEDR functionality and a KEDR license key has been added.

# Recommendations for processing YARA alerts

In the right part of the window, the **Recommendations** section displays recommendations that you can follow, as well as the number of alerts or events that have attributes in common with the alert you are working on.

*You can follow the following recommendations:*

- Under **Qualifying**, expand the **Find related alerts** list.

A list of attributes is displayed that can be used to find similar alerts, and the number of similar alerts for each attribute.

Select one of the following attributes:

- **By MD5**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the MD5 hash. The MD5 hash of the file from the alert you are working on is highlighted in yellow.
- **By SHA256**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the SHA256 hash. The SHA256 hash of the file from the alert you are working on is highlighted in yellow.
- **By host name**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The host name from the alert you are working on is highlighted in yellow.
- **By sender address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The sender address of the email message from the alert you are working on is highlighted in yellow.
- **By recipient address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Destination** column. The recipient address of the email message from the alert you are working on is highlighted in yellow.
- **By URL**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the URL from the alert you are working on.

- Under **Qualifying**, select **Find related KES events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the **Detect processing result** event type is selected and a search filter is configured, for example, by **RemoteIP**, **MD5**, **SHA256**, **URI**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

  The action is only available if you are using KEDR functionality and a KEDR license key has been added.

- Under **Investigation**, select **Find related events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, a search filter is configured, for example, by **RemoteIP**, **MD5**, **SHA256**, **URI**. The filtering values are populated with the properties of the alert you are working on. For example, the MD5 hash of the file in the alert.

  The action is only available if you are using KEDR functionality and a KEDR license key has been added.

# Recommendations for processing IOC alerts

In the right part of the window, the **Recommendations** section displays recommendations that you can follow, as well as the number of alerts that have attributes in common with the alert you are working on.

*You can follow the following recommendations:*

- Under **Qualifying**, select **Find related alerts by host name**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The host name from the alert you are working on is highlighted in yellow.
- Under **Qualifying**, select **Find related alerts by IOC**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Detected** column, the name of the IOC file from the alert you are working on.
- In the **Quick response** section, select **Isolate <host name>**. This opens the network isolation rule creation window.

*To create a host isolation rule, enter the following settings:*

1. In the **Disable isolation in** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.
2. In the **Exceptions to the host isolation rule** settings group, in the **Traffic direction** list, select the direction of network traffic that must not be blocked:
   - **Incoming/Outgoing**.
   - **Incoming**.
   - **Outgoing**.
3. In the **IP** field, enter the IP address whose network traffic must not be blocked.
4. If you selected **Incoming** or **Outgoing**, in the **Ports** field enter the connection ports.
5. If you want to add more than one exclusion, click **Add server** and repeat the steps to fill in the **Traffic direction**, **IP** and **Ports** fields.
6. Click **Save**.

# Recommendations for processing IDS alerts

In the right part of the window, the **Recommendations** section displays recommendations that you can follow, as well as the number of alerts or events that have attributes in common with the alert you are working on.

*You can follow the following recommendations:*

- Under **Qualifying**, select **Find related alerts by host name**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Update source** column. The host name or IP address from the alert you are working on is highlighted in yellow.
- Under **Qualifying**, select **Find related alerts by URL**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Details** column, the URL. The URL from the alert you are working on is highlighted in yellow.
- Under **Qualifying**, select **Add to exceptions**.

  This opens the **Add IDS rule to exceptions** window. If you want to add an IDS rule that was used to create the alert to exclusions, enter a comment in the **Description** field and click **Add server**.

The IDS rule is added to exclusions and is displayed in the exclusion list in the **Program settings** section, **White lists** subsection on the **IDS exceptions** in the program web interface.

- Under **Investigation**, select **Find related events by URL**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the search filter is configured to use the **URI** from the alert you are working on.
- Under **Investigation**, select **Find related events by host name**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the search filter is configured to use the **RemoteIP** from the alert you are working on.
- In the **Investigation** section, click **Download IDS artifact** to download the file with alert data.
- In the **Investigation** section, click **Download PCAP file** to download the file with intercepted traffic data.

# 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.
- 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.
- Add a comment to an alert.

  You can find commented alerts based on keywords within comments by filtering alerts based on received information.
- 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.

# 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.

   This opens the table of alerts.
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.

   This opens the action confirmation window.

5. Click **Proceed**.

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.

# 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.

   This opens the table of alerts.

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. This opens the action confirmation window.

   You can also leave a comment that will be displayed in the alert change history.

5. Click **Proceed**.

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.

   This opens the table of alerts.

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.

   This opens the table of alerts.

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.

   This opens the table of alerts.

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.

   This opens the action confirmation window.

   You can also leave a comment that will be displayed in the alert change history.

4. Click **Proceed**.

   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.

# 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.

   This opens the table of alerts.

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.

   This opens the action confirmation window.

   You can also leave a comment that will be displayed in the alert change history.

4. Click **Proceed**.

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.

## 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.

   This opens the table of alerts.

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.

# Events database threat hunting

When managing the program web interface, users with the **Senior security officer** and **Security officer** roles can generate search queries and use IOC files and TAA (IOA) rules to search the events database for threats, for organizations whose data they are allowed to access.

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, you can create and modify search queries using text commands.

You can upload an IOC file and search for events based on conditions defined in this IOC file.

You can also create TAA (IOA) rules based on event search conditions.

# Searching events in design mode

*To define event search conditions in design mode:*

1. Select the **Threat Hunting** section, **Builder** tab in the program web interface window.
   This opens the event search form.
2. In the drop-down list, select the criterion for searching for events in one of the following groups:
   - **General details**.
   - **TAA properties**.
   - **File properties**.
   - **Process started**.
   - **Remote connection**.
   - **Registry modified**.
   - **Windows Log event**.
   - **Host name changed**.
   - **Detect and processing result**.
   - **Console interactive input**.
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.

4. 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.
5. If you want to add a new condition, use the **AND** or **OR** logical operator and repeat the necessary actions for adding a condition.
6. If you want to add a group of conditions, click the **Group** button and repeat the actions necessary for adding conditions.
7. If you want to delete a group of conditions, click the **Remove group** button.
8. 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.
9. 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 **Apply**.

   The calendar closes.
10. Click **Search**.

The table of events that satisfy the search criteria is displayed.

# Searching events in 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 **Apply**.

   The calendar closes.

5. Click **Search**.

The table of events that satisfy the search criteria is displayed.

# 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.

   The table of events that satisfy the search criteria is displayed.

# Searching events by processing results in EPP programs

*To search events by processing results in EPP programs in design mode:*

1. Select the **Threat Hunting** section, **Builder** tab in the program web interface window.
   This opens the event search form.
2. To search events by processing status:
   a. In the search criteria drop-down lost in the **Detect and processing result** group, select **ThreatStatus**.
   b. In the drop-down list of comparison operators, select one of the following options:
      - **=** (equals);
      - **!=** (does not equal).
   c. In the drop-down list of event processing status, select one of the following options:
      - **Object clean**.
      - **Object disinfected**.
      - **False positive**.
      - **Object added by user**.
      - **Object added to exceptions**.
      - **Object deleted**.
      - **Object quarantined**.
      - **Object not found**.
      - **Object rolled back**.
      - **Object cannot be processed**.
      - **Object not processed**.
      - **Processing terminated**.
      - **Unknown**.

3. To search events by reasons why they were not processed:

   a. In the search criteria drop-down lost in the **Detect and processing result** group, select **UntreatedReason**.

   b. In the drop-down list of comparison operators, select one of the following options:

   - **=** (equals);
   - **!=** (does not equal).

   c. In the drop-down list of reasons why the events were not processed, select one of the following options:

   - **Object already processed**.
   - **Application runs in Report only mode**.
   - **Failed to backup object**.
   - **Failed to copy object**.
   - **Device not ready**.
   - **Object locked**.
   - **No rights to perform action**.
   - **Object not curable**.
   - **Object not overwritable**.
   - **Object not found**.
   - **Disk out of space**.
   - **Processing canceled**.
   - **Processing postponed**.
   - **Processing task stopped**.
   - **Data read error**.
   - **Reason unknown**.
   - **Object is critical system**.
   - **Data write error**.
   - **Data write not supported**.
   - **Object write-protected**.

4. If you want to add a new condition, use the **AND** or **OR** logical operator and repeat the necessary actions for adding a condition.

5. If you want to add a group of conditions, click the **Group** button and repeat the actions necessary for adding conditions.

6. If you want to delete a group of conditions, click the **Remove group** button.

7. 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.

8. 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 **Apply**.

   The calendar closes.

9. Click **Search**.

The table of events that satisfy the search criteria is displayed.

# 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.

   This opens the event search form.

2. Click **Import**.

   This opens the file selection window.

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.

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 **Apply**.

   The calendar closes.

6. Click **Search**.

An event table is displayed that corresponds to criteria specified in the IOC file.

# Creating a user-defined TAA (IOA) rule based on event search conditions

*To create a user-defined TAA (IOA) based on event search conditions:*

1. Select the **Threat Hunting** section in the program web interface window.
   This opens the event search form.
2. Perform an event search in design mode or source code mode.
3. Click the **Save as TAA (IOA) rule** button.
   This opens the **New TAA (IOA) rule** window.
4. In the **Name** field, type the name of the rule.
5. Click **Save**.

   The event search condition will be saved. In the TAA (IOA) rule table in the **User rules** section, **TAA** subsection of the web interface, the new rule is displayed with the specified name.

If you want to save event search conditions as a user-defined TAA (IOA) rule, avoid using the following fields:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.

- IOAImportance.
- IOAConfidence.

At the time of saving the user-defined TAA (IOA) rule, the program might not have any events containing data for these fields. When events with this data turn up, the user-defined field that you have created earlier will be unable to mark events by these fields.

# 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.

Event information displays local timestamps of the Kaspersky Endpoint Agent computer that detected the event. The program administrator must make sure the time on Kaspersky Endpoint Agent computers is current.

If you are using the distributed solution and multitenancy mode, the section displays data on the organization that you chose.

*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.

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. **Host**—Name of the computer on which the event was detected.
4. **Details**—Information about the event.
5. **User name**—Name of the user on the computer with Kaspersky Endpoint Agent whose user account was used to detect the event.

Each type of event has its own type of cell value in the **Details** column of the events table (see the table below).

Correspondence of the types of cell values in the **Details** and **Event** columns

| Event | Details |
|---|---|
| **Process started** | Name of the process file that was started. SHA256- and MD5 hash. Event importance. |
| **Module loaded** | Name of the dynamic library that was loaded. SHA256- and MD5 hash. Event importance. |
| **Remote connection** | IP address or URL to which a remote connection attempt was made. Name of the file that attempted to establish a remote connection. Event importance. |
| **Prevention rule** | Name of the file of the application that was blocked from starting. SHA256- and MD5 hash. Event importance. |
| **Document blocked** | Name of the document that was blocked from starting. SHA256- and MD5 hash. Event importance. |
| **File created** | Name of the created file. SHA256- and MD5 hash. Event importance. |
| **Windows Log event** | Event importance. |
| **Registry modified** | Name of key in registry. `<name of the variable in the key>=<value of the variable>.` Event importance. |
| **Port listened** | Server address and port. Name of the file of the process that listens to the port. Event importance. |
| **Driver loaded** | File name of the driver that has been loaded. SHA256- and MD5 hash. Event importance. |
| **Detect** | Path to the detected file. SHA256- and MD5 hash. Category of the detected object (for example, name of a virus). Event importance. |
| **Detect processing result** | Path to the detected file. SHA256- and MD5 hash. Category of the detected object (for example, name of a virus). Event importance. |
| **Interpreted file run** | Event importance. |
| **Console interactive input** | Event importance. |

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 KL TIP**.
  - **Create a prevention rule**.
  - **Find in Storage**.

- SHA256 hash:
  - **Find on KL TIP**.
  - **Find on virustotal.com**.
  - **Create a prevention rule**.
  - **Find in Storage**.

# Viewing information about an event

*To view information about an event:*

1. In the program web interface window, select the **Threat Hunting** section, **Builder** or **Source code** tab.

   This opens the event search form.

2. 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 in design mode or source code mode.

   The event table is displayed.

4. Select the event whose information you want to view.

This opens a window containing information about the event.

# Information about events in the tree of events

The tree of events is displayed in the upper part of the event information window.

The tree of events contains the following information:

- The event for which you are viewing information.

  The event you are viewing is displayed on the right side.

- The parent process.

  The parent process is displayed to the left of the event you are viewing. If the event you are viewing does not have a parent process, the host name where the event was registered is displayed instead.

Clicking the name of the parent process on the left side displays the process that has initiated the process in question and is a parent process with regard to that process. If there is no parent process, the host name is displayed instead.

To the right of each parent process name, the total number of events generated by this process is displayed. You can view the list of events and information about the selected event.

## Viewing parent process information in the tree of events

*To display parent process information for the event being viewed:*

1. Perform an event search in design mode or source code mode.

   The event table is displayed.

2. Select the event whose information you want to view.

   This opens a window containing information about the event. The upper part of the window displays the tree of events.

3. Click the name of the parent process.

   In the bottom part of the window, the **Details** tab displays information about the process that is the parent process with regard to the event being viewed.

## Viewing information about events initiated by the parent process in the tree of events

*To display a table of all events initiated by the parent process:*

1. Perform an event search in design mode or source code mode.

   The event table is displayed.

2. Select the event whose information you want to view.

   This opens a window containing information about the event. The upper part of the event information window displays the tree of events.

3. Click the name of the parent process in the event tree.

   In the bottom part of the window, the **Details** tab displays information about the event that is the parent event with regard to the event being viewed.

4. Go to the **Events** tab.

   A table of all events initiated by the parent process is displayed. By default, events in the table are sorted by time, with the newest events at the top of the table.

   You can view event information by clicking the row of the relevant event. The event node is displayed in the tree of events.

*To display the event table grouped by type:*

1. Perform an event search in design mode or source code mode.

   The event table is displayed.

2. Select the event whose information you want to view.

   This opens a window containing information about the event. The upper part of the event information window displays the tree of events.

3. Click the drop-down list to the right of the parent process name in the tree of events.

   A list of all events initiated by the parent process is displayed. By default, the events in the list are grouped by type.

4. In the tree of events, in the drop-down list to the right of the parent process name, select one of the following options:

   - If you want to display all events initiated by the parent process, click **All events**.

     A table of all events initiated by the parent process is displayed. By default, events in the table are sorted by time, with the newest events at the top of the table.

   - If you want to view all events of a particular type initiated by the parent process, select the name of the relevant event type.

     A table of all events initiated by the parent process is displayed, grouped by type.

   You can view event information by clicking the row of the relevant event. The event is displayed in the tree of events.

## Viewing host information in the tree of events

If the event that you are viewing or the parent process do not have a process that initiated it, the process node in the tree of events is replaced with the node of the host where the event was registered or the parent process was running.

*To view information for the host where the event was registered or the parent process was running:*

1. Perform an event search in design mode or source code mode.

   The event table is displayed.

2. Select the event whose information you want to view.

   This opens a window containing information about the event. The upper part of the window displays the tree of events.

3. Click the host name in the tree of events.

   The bottom part of the window displays information about the host where the event was registered or the parent process was running.

# Recommendations for processing events

The event window displays recommendations for processing the event in the box between the event tree and the information text.

You can follow the following recommendations:

- **Isolate <host name>**—isolate the host with Endpoint Agent where the event was detected from the network. For all event types.
- **Create a prevention rule**—prohibit the execution of the file that was detected in the event. For all event types except **Windows Log event** and **Host name changed**.
- **Create a task**—create a task. For all event types except **Windows Log event** and **Host name changed**.

Additionally, you can process the event by clicking the link with the name, path, MD5 or SHA256 hash of the file and the host name while viewing text information about the event in the lower part of the window.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- **Find alerts**.
- Run the following tasks:
  - **Kill process**.
  - **Kill unique process**.
  - **Delete file**.
  - **Get file**.
  - **Quarantine file**.
  - **Run program**.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- **Find events**.
- **Find alerts**.
- **Find on KL TIP**.
- **Find in Storage**.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- **Find events**.
- **Find alerts**.

- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

## Following a recommendation to isolate a host

*To follow a recommendation to isolate a host from the network:*

1. In the recommendation box, select **Isolate <host name>**.

   This opens the host isolation settings window for the host from the event you are working on.

2. In the **Disable isolation in** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.

3. In the **Exceptions to the host isolation rule** settings group, in the **Traffic direction** list, select the direction of network traffic that must not be blocked:

   - **Incoming/Outgoing**.
   - **Incoming**.
   - **Outgoing**.

4. In the **IP** field, enter the IP address whose network traffic must not be blocked.

5. If you selected **Incoming** or **Outgoing**, in the **Ports** field enter the connection ports.

6. If you want to add more than one exclusion, click **Add server** and repeat the steps to fill in the **Traffic direction**, **IP** and **Ports** fields.

7. Click **Save**.

Information about host isolation is displayed in the **Endpoint Agents** section of the web interface.

You can also create a network isolation rule by clicking the **Isolate <host name>** link in the alert information and in the **Endpoint Agents** section of the web interface.

# Following a recommendation to prevent a file from running

*To follow a recommendation to prevent a file from running:*

1. In the recommendations box, select **Create a prevention rule**.

   This opens the prevention rule creation window with the MD5 or SHA256 hash of the file from the event you are working on.

2. Configure the following settings:

   a. **State** is the state of the prevention rule:

   - If you want to enable the prevention rule, set the toggle switch to **On**.
   - If you want to disable the prevention rule, set the toggle switch to **Off**.

   b. **Name** is the name of the prevention rule.

   c. 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.

   d. If you want to change the scope of the prevention rule, configure the **Prevent on** setting:

   - 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.

3. Click the **Add** button.

The file run prevention is created.

Information about the created prevention is displayed in the **Prevention** section of the web interface.

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.

# Following a recommendation to create a task

*To follow a recommendation to create a task:*

1. Click **Create a task**, and in the recommendation box, expand the list of task types.
2. Select a task type:
   - **Kill process**.
   - **Kill unique process**.
   - **Delete file**.
   - **Get file**.
   - **Quarantine file**.

   This opens the task creation window with preset values (for example, host name, file path, MD5 or SHA256 hash of the file) from the event you are working on.
3. If you want to modify preset values from the event, edit the corresponding fields.
4. If you want to add a comment for the task, enter it in the **Description** box.
5. If you are creating a **Kill process** or **Delete file** task and you want to modify the scope of the task, change the value of the **Task for** setting:
   - 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.
6. Click the **Add** button.

The task is created.

Information about the created task is displayed in the **Tasks section** of the web interface.

# Information about the "Process started" event

The window showing information about **Process started** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Process started** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Process start time.
  - **File**—Process file name.
  - **Launch parameters**—Process startup settings.
  - **Process end time**—Time when the process was terminated.
  - **Process ID**—Process identifier.
  - **Account type**—Type of the account that ran the process. For example, administrator.
  - **Logon type**—Method used to log on to the system.
  - **Host name**—Name of the Endpoint Agent host on which the process was started.
  - **User name**—Name of the user that started the process.
- **Parent process** section:
  - **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.
- **File** section:
  - **MD5**—MD5 hash of the process file.
  - **SHA256**—SHA256 hash of the process file.
  - **Size**—Size of the process file.

- **Program name**. For example, name of the operating system.
- **Vendor**. For example, vendor of the operating system.
- **File description**. For example, Example File.
- **Original file name**. For example, ExampleFile.exe.
- **Signature organization**—Organization that issued the digital certificate of the file.
- **Signature validation result**. For example, signature invalid or signature OK.
- **Attributes**—File attribute in accordance with the Windows classification. For example, A (archive), D (directory), or S (system file).
- **Time created**—Process file creation time.
- **Time modified**—Time of last modification of the process file.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.

- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Module loaded" event

The window showing information about **Module loaded** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Module loaded** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time when the module was loaded.
  - **File**—Name 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.
- **Parent process** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

- **File** section:
  - **MD5**—MD5 hash of the loaded module file.
  - **SHA256**—SHA256 hash of the loaded module file.
  - **Size**—Size of the loaded module.
  - **Program name**. For example, name of the operating system.
  - **Vendor**. For example, vendor of the operating system.
  - **File description**. For example, Example File.
  - **Original file name**. For example, ExampleFile.exe.
  - **Signature organization**—Organization that issued the digital certificate of the file.
  - **Signature validation result**. For example, signature invalid or signature OK.
  - **Time created**—Creation time of the loaded module.
  - **Time modified**—Date of last modification of the loaded module.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Remote connection" event

The window showing information about **Remote connection** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Remote connection** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time of the remote connection attempt.
  - **Connection direction**—Direction of the connection (Incoming or Outgoing).
  - **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** section:
  - **File**—Name of the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

Clicking the link with the file name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Prevention rule" event

The window with information about events in which prevention rules were triggered, i. e. events of the **Prevention rule** type, displays the following details:

- Tree of events.
- Recommendations for processing an event.
- **Prevention rule** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **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.
  - **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** section:
  - **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.

- **File** section:
  - **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.
  - **Program name**. For example, name of the operating system.
  - **Vendor**. For example, vendor of the operating system.
  - **File description**. For example, Example File.
  - **Original file name**. For example, ExampleFile.exe.
  - **Signature organization**—Organization that issued the digital certificate of the file.
  - **Signature validation result**. For example, signature invalid or signature OK.
  - **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.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Document blocked" event

The window showing information about **Document blocked** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Document blocked** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time when the document was blocked.
  - **File**—Name of the blocked document.
  - **MD5**—MD5 hash of the blocked document.
  - **SHA256**—SHA256 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.
- **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** section:
  - **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.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.

- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "File created" event

The window showing information about **File created** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **File created** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **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** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Windows log event" event

The window showing information about **Windows Log event** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Windows Log event** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time when the event was detected.
  - **Security event ID**—Identifier of the type of security event in the Windows log.
  - **Host name**—Name of the host on which the event occurred.
- **System** and **EventData** settings groups containing data from the Windows system log. The scope of data depends on the type of Windows event.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Find on KL TIP.

- Run the following tasks:
  - **Kill process**.
  - **Kill unique process**.
  - **Delete file**.
  - **Get file**.
  - **Quarantine file**.
  - **Run program**.
- **Copy value to clipboard**.

## Information about the "Changes in the registry" event

The window showing information about **Registry modified** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Registry modified** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **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** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

Clicking the link with the file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Find on KL TIP.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.

- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Port listened" event

The window showing information about **Port listened** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Port listened** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Port listening time.
  - **Local 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** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

Clicking the link with the file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Find on KL TIP.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.

- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Driver loaded" event

The window showing information about **Driver loaded** events contains the following details:

- Tree of events.
- **Driver loaded** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time when the driver was loaded.
  - **File**—Name of the loaded driver file.
  - **Host name**—Name of the host on which the driver was loaded.
- **File** section:
  - **MD5**—MD5 hash of the loaded driver file.
  - **SHA256**—SHA256 hash of the loaded driver file.
  - **Size**—Size of the loaded driver.
  - **Time created**—Creation time of the loaded driver.
  - **Time modified**—Time of last modification of the loaded driver.
  - **Program name**. For example, name of the operating system.

- **Vendor**. For example, vendor of the operating system.
- **File description**. For example, Example File.
- **Original file name**. For example, ExampleFile.exe.
- **Signature organization**—Organization that issued the digital certificate of the file.
- **Signature validation result**. For example, signature invalid or signature OK.
- **Time created**—Creation time of the loaded driver.
- **Time modified**—Date of last modification of the loaded driver.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.

- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Information about the "Alert" event

The window showing information about a **Detect** type event contains the following details:

- Tree of events.
- On the **Details** tab, under **Detect**:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Date and time of the event.
  - **Detect**—Name of the detected object. Clicking the link with the object name opens a list in which you can select one of the following actions:
    - **Find events**—Find all events in which this object was detected.
    - **View on Kaspersky Threats Portal**.
    - **Copy value to clipboard**.
  - **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.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Kaspersky Anti Targeted Attack Platform generates a **Detect** event based on data received from EPP programs. If EPP programs are not installed on the computer and are not integrated with Kaspersky Endpoint Agent, information about the **Detect** event is not logged in the event database and is not displayed in the program web interface.

# Information about the "Alert processing result" event

The window showing information about a **Detect processing result** type event contains the following details:

- Tree of events.
- On the **Details** tab, under **Detect processing result**:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Date and time of the event.
  - **Detect**—Name of the detected object. Clicking the link with the object name opens a list in which you can select one of the following actions:
    - **Find events**—Find all events in which this object was detected.
    - **View on Kaspersky Threats Portal**.
    - **Copy value to clipboard**.
  - **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.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
    - Kill process.
    - Kill unique process.
    - Delete file.
    - Get file.
    - Quarantine file.
    - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

The Kaspersky Anti Targeted Attack Platform server generates a **Detect processing result** event based on data received from EPP programs. If EPP programs are not installed on the computer and are not integrated with the Endpoint Agent component, information about the **Detect processing result** event is not logged in the event database and is not displayed in the program web interface.

# Information about the "Interpreted file run" event

The window showing information about **Interpreted file run** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Interpreted file run** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time when the event was detected.
  - **File**—Name of the file.
  - **MD5**—MD5 hash of a file.
  - **SHA256**—SHA256 hash of a file.
  - **Size**—Size of the 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 run.
- **User name**—Name of the user whose account was used to run the file.

- **Parent process** section:
  - **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.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.

- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

## Information about the "Interactive command input at the console" event

The window showing information about **Console interactive input** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Console interactive input** section:
  - **IOA tags**—Information about the results of file analysis using the Targeted Attack Analyzer technology: name of the TAA (IOA) rule that was used to create the alert.

    Click the link to display information about the TAA (IOA) rule. If the rule was provided by Kaspersky experts, it contains information about the triggered MITRE technique as well as recommendations for reacting to the event.
  - **Event time**—Time when the event was detected.
  - **Input text**—Text entered at the command line (for example, CMD) on the host with the Kaspersky Endpoint Agent for Windows program.
  - **Host name**—Name of the host on which the command was entered.
  - **User name**—Name of the user whose account was used to enter the command.
- **Parent process** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- Find in Storage.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find in Storage.

- **Create a prevention rule**.
- **Copy value to clipboard**.

# Managing Kaspersky Endpoint Agent host information

Kaspersky Endpoint Agent 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 Kaspersky Endpoint Agent is installed, on the **Endpoint Agents** tab of the program web interface window for organizations whose data the user is allowed to access. If you are using distributed solution and multitenancy mode, the web interface of the PCN server displays the list of hosts with Kaspersky Endpoint Agent 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 Kaspersky Endpoint Agent installed, for organizations whose data they are allowed to access.

If suspicious network activity is detected, users with the **Senior security officer** role can isolate from the network any host with Kaspersky Endpoint Agent, for organizations whose data the user is allowed to access. In this case, the connection between the server with the Central Node component and a host with Kaspersky Endpoint Agent is not interrupted.

To provide support in case of problems with Kaspersky Endpoint Agent, Technical Support staff 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 obtained for debugging purposes. The extended diagnostic information that is obtained is saved on the user's computer. The retrieved data is not automatically sent to Kaspersky.

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 Kaspersky Endpoint Agent host table on a standalone Central Node server

The table of hosts with Kaspersky Endpoint Agent installed is located in the **Endpoint Agents** section of the program web interface window.

If you are using a standalone Central Node server, but not using distributed solution and multitenancy mode, the table of Kaspersky Endpoint Agent hosts can display the following data:

- Number of hosts and activity indicators of Kaspersky Endpoint Agent:
  - **Critical inactivity** is the number of hosts from which latest data was received a very long time ago.
  - **Warning** is the number hosts from which latest data was received a long time ago.
  - **Normal activity** is the number of hosts from which latest data was recently received.
- **Host**—Name of the host with Kaspersky Endpoint Agent.
- **IP**—IP address of the host where Kaspersky Endpoint Agent is installed.
- **OS**—Version of the operating system that is installed on the computer with Kaspersky Endpoint Agent.
- **Version**—Version of Kaspersky Endpoint Agent installed.
- **Activity**—Activity indicator of Kaspersky Endpoint Agent. 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 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**.
- Run the following tasks:
  - Kill process.
  - Kill unique process.
  - Delete file.
  - Get file.
  - Quarantine file.
  - Run program.

- New prevention rule.
- Isolate from network.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

Clicking the link with the IP opens a list in which you can select one of the following actions:

- **Filter by this value**.
- **Exclude from filter**.
- Find alerts.
- **Copy value to clipboard**.

Clicking a link in any other 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 Kaspersky Endpoint Agent host table in distributed solution and multitenancy mode

The table of Kaspersky Endpoint Agent hosts is located in the **Endpoint Agents** section of the program web interface window.

If you are using the distributed solution and multitenancy mode, the table contains information about Kaspersky Endpoint Agent hosts connected to the PCN and all SCN servers. The table can display the following data:

- Number of hosts and activity indicators of Kaspersky Endpoint Agent:
  - **Critical inactivity** is the number of hosts from which latest data was received a very long time ago.
  - **Warning** is the number hosts from which latest data was received a long time ago.
  - **Normal activity** is the number of hosts from which latest data was recently received.
- **Host** is the name of the host with Kaspersky Endpoint Agent.

  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 Kaspersky Endpoint Agent host is connected.
- **IP**—IP address of the computer where Kaspersky Endpoint Agent is installed.
- **OS**—Version of the operating system that is installed on the computer with Kaspersky Endpoint Agent.
- **Version**—Version of Kaspersky Endpoint Agent installed.
- **Activity**—Activity indicator of Kaspersky Endpoint Agent. 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 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**.
- Run the following tasks:
    - Kill process.
    - Kill unique process.
    - Delete file.
    - Get file.
    - Quarantine file.
    - Run program.
- New prevention rule.
- Isolate from network.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

Clicking the link with the IP opens a list in which you can select one of the following actions:

- **Filter by this value**.
- **Exclude from filter**.
- Find alerts.
- **Copy value to clipboard**.

Clicking a link in any other 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 information about a host

*To view information about a host with Kaspersky Endpoint Agent:*

1. Select the **Endpoint Agents** 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:

- Recommendations group:
  - Clicking the **Alerts** link opens the **Alerts** section with the search condition containing the selected host.
  - Clicking the **Events** link opens the **Threat Hunting** section with the search condition containing the selected host.
  - Clicking the **Events affected by prevention rules** link opens the **Threat Hunting** section with the search condition containing the selected host and the **Prevention rule** event type.
- The **Details** tab:
  - In the **Host** section:
    - **Name**—Name of the computer with Kaspersky Endpoint Agent.
    - **IP**—IP address of the host where Kaspersky Endpoint Agent is installed.
    - **OS**—Version of the operating system on the host with the Kaspersky Endpoint Agent program installed.
    - **Server**—Name of the SCN or PCN server. Only displayed in distributed solution and multitenancy mode.

- In the **TLS certificate for Kaspersky Endpoint Agent connection** section:
  - **Endpoint Agent version**—Version of Kaspersky Endpoint Agent installed.
  - **Activity**—Activity indicator of Kaspersky Endpoint Agent. 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.
  - **Connected to server**—Name of the Central Node, SCN, or PCN server to which the host is connected.
  - **Last connection**—time of the last connection to the Central Node, SCN, or PCN server.
  - **License key status**—Information about the Kaspersky Endpoint Agent license key.
- The **Prevention** tab, where you can see MD5 or SHA256 hashes for files that were prevented from running or opening on the host. The following information is displayed:
  - **Name**—Name of the file.
  - **State**—State of the prevention rule.
  - **Hash**—Hashing algorithm.
- The **Tasks** tab where you can see which tasks were run on the host. The following information is displayed:
  - **Time created**—Task creation date and time.
  - **Name**—Task name.
  - **Details**—Full path to the file or data stream for which the task was created.
  - **State**—Task completion status.

Clicking the link with the host name opens a list in which you can select one of the following actions:

- Run the following tasks:
  - **Kill process**.
  - **Delete file**.
  - **Get file**.
  - **Quarantine file**.
  - **Run program**.
- **New prevention rule**.
- **Isolate from network**.
- **Find events**.

- Find alerts.
- **Copy value to clipboard**.

Clicking the link with the IP opens a list in which you can select one of the following actions:

- Find alerts.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- **Filter by this value**.
- **Exclude from filter**.
- Find on KL TIP.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

Clicking the **SHA256** link opens a list in which you can select one of the following actions:

- **Filter by this value**.
- **Exclude from filter**.
- Find on KL TIP.
- **Find on virustotal.com**.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

# Filtering and searching hosts with Kaspersky Endpoint Agent by host name

*To filter or search for hosts with the Kaspersky Endpoint Agent program by host name:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Host** link to open the filter configuration window.
3. If you want to display only isolated hosts, select the **Show isolated Endpoint Agents only** check box.

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 host name.
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 **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent that have been isolated from the network

*To filter or search for hosts with the Kaspersky Endpoint Agent program that are isolated from the network:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Host** link to open the filter configuration window.
3. Select the **Show isolated Endpoint Agents only** check box.
4. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by PCN and SCN server names

If you are using distributed solution and multitenancy mode, you can filter or find hosts with the Kaspersky Endpoint Agent program based on the names of PCN and SCN servers to which those hosts are connected.

*To filter or search for hosts with the Kaspersky Endpoint Agent program by the names of PCN and SCN servers:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

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 Kaspersky Endpoint Agent program.

4. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by computer IP address

*To filter or search for hosts with the Kaspersky Endpoint Agent program based on the IP address of the computer with the Kaspersky Endpoint Agent program installed:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

2. Click the **IP** link to open the filter configuration window.

3. In the drop-down list, select one of the following filtering operators:

   - **Contains**.
   - **Does not contain**.

4. 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`).

5. To add a filter condition using a different criterion, click + and specify the filter condition.

6. If you want to delete the filter condition, click the button to the right of the field.

7. Click **Apply**.

The filter configuration window closes.

The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by operating system version on the computer

*To filter or search for hosts with the Kaspersky Endpoint Agent program based on the version of the operating system installed on the computer hosting the Kaspersky Endpoint Agent program:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

2. Click the **OS** link to open the filter configuration window.

3. In the drop-down list, select one of the following filtering operators:

   - **Contains**.
   - **Does not contain**.

4. In the entry field, specify one or several characters of the operating system version.

5. To add a filter condition using a different criterion, click + and specify the filter condition.

6. If you want to delete the filter condition, click the button to the right of the field.

7. Click **Apply**.

The filter configuration window closes.

The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent by Kaspersky Endpoint Agent version

*To filter or search for hosts with the Kaspersky Endpoint Agent program based on the version of the Kaspersky Endpoint Agent program:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Version** link to open the filter configuration window.
3. In the drop-down list, select one of the following filtering operators:
   - **Contains**.
   - **Does not contain**.
4. In the entry field, specify one or several characters of the version of the Kaspersky Endpoint Agent program.
5. To add a filter condition using a different criterion, click + and specify the filter condition.
6. If you want to delete the filter condition, click the button to the right of the field.
7. Click **Apply**.

   The filter configuration window closes.

   The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Filtering and searching hosts with Kaspersky Endpoint Agent based on their activity

*To filter or search for hosts with the Kaspersky Endpoint Agent program by their activity:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
   This opens the table of hosts.
2. Click the **Activity** link to open the filter configuration window.

3. Select the check boxes next to one or more Kaspersky Endpoint Agent program activity indicators:

   - **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.

4. Click **Apply**.

The filter configuration window closes.

The table displays only those hosts that match the filter criteria you have set.

You can use multiple filters at the same time.

# Quickly creating a filter for hosts with Kaspersky Endpoint Agent

*To quickly create a filter for hosts with the Kaspersky Endpoint Agent program:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

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 displays only those hosts that match the filter criteria you have set.

# Resetting the hosts with Kaspersky Endpoint Agent filter

*To clear a filter for hosts with Kaspersky Endpoint Agent program based on one or multiple filter conditions:*

1. Select the **Endpoint Agents** section in the window of the program web interface.
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 displays only those hosts that match the filter criteria you have set.

# Supported interpreters and processes

Kaspersky Endpoint Agent program monitors the execution of scripts by the following interpreters:

- cmd.exe;
- reg.exe;
- regedit.exe;
- regedt32.exe;
- cscript.exe;
- wscript.exe;
- mmc.exe;
- msiexec.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 Kaspersky Endpoint Agent program is presented in the table below.

Processes and the file extensions that they open

| Process | File extensions |
|---|---|
| winword.exe | rtf<br>doc<br>dot<br>docm<br>docx<br>dotx<br>dotm<br>docb |
| excel.exe | xls<br>xlt<br>xlm<br>xlsx<br>xlsm<br>xltx<br>xltm<br>xlsb<br>xla<br>xlam<br>xll<br>xlw |
| powerpnt.exe | ppt<br>pot<br>pps<br>pptx<br>pptm<br>potx<br>potm<br>ppam<br>ppsx<br>ppsm<br>sldx<br>sldm |
| acrord32.exe | pdf |
| wordpad.exe | docx<br>pdf |

| Process | File extensions |
| --- | --- |
| chrome.exe | pdf |
| MicrosoftEdge.exe | pdf |

# Network isolation of Kaspersky Endpoint Agent hosts

When responding to threats, users with the **Senior security officer** role can isolate hosts with detected objects that require your attention when investigating the incident.

Network isolation is available for hosts with Kaspersky Endpoint Agent version 3.8 or newer.

Network isolation is not a Threat Response action by itself. The security officer should take steps to investigate the incident on his own while the network isolation is active for the host. You can configure the duration of host network isolation when you create the network isolation 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 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.

In cases when Kaspersky Endpoint Agent is turned off on the host, and also for a certain period of time after turning on Kaspersky Endpoint Agent or rebooting the computer with Kaspersky Endpoint Agent, network isolation of the host may be inactive.

You can also manage network isolation using the the Kaspersky Security Center Administration Console. It is recommended to manage network isolation either only in Kaspersky Security Center or only in Kaspersky Anti Targeted Attack Platform. Correct functioning is not guaranteed when managing network isolation from the interface of both programs.

Some limitations apply when network isolation is used.

# Creating a network isolation rule

*To create a network isolation rule:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

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 **Isolate**.

4. In the **Disable isolation in** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.

5. In the **Exceptions to the host isolation rule** settings group, in the **Traffic direction** list, select the direction of network traffic that must not be blocked:

   - **Incoming/Outgoing**.
   - **Incoming**.
   - **Outgoing**.

6. In the **IP** field, enter the IP address whose network traffic must not be blocked.

7. If you selected **Incoming** or **Outgoing**, in the **Ports** field enter the connection ports.

8. If you want to add more than one exclusion, click **Add server** and repeat the steps to fill in the **Traffic direction**, **IP** and **Ports** fields.

9. Click **Save**.

The host will be isolated from the network.

You can also create a network isolation rule by clicking the **Isolate <host name>** link in the event information and in the alert information.

# Adding an exclusion from a network isolation rule

*To add an exclusion to a previously created network isolation rule:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

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 exceptions** link to expand the **Exceptions to the host isolation rule** settings group.

4. In the **Disable isolation in** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.

5. In the **Exceptions to the host isolation rule** settings group, in the **Traffic direction** list, select the direction of network traffic that must not be blocked:

   - **Incoming/Outgoing**.
   - **Incoming**.
   - **Outgoing**.

6. In the **IP** field, enter the IP address whose network traffic must not be blocked.

7. If you selected **Incoming** or **Outgoing**, in the **Ports** field enter the connection ports.

8. If you want to add more than one exclusion, click **Add server** and repeat the steps to fill in the **Traffic direction**, **IP** and **Ports** fields.

9. Click **Save**.

The network isolation rule exclusion will be added.

# Deleting a network isolation rule

*To delete a network isolation rule:*

1. Select the **Endpoint Agents** section in the window of the program web interface.

   This opens the table of hosts.

2. Click the name of the host for which you want to delete a network isolation rule to open the action menu for the host.

3. Select the **Delete host isolation rule** action.

   This opens the action confirmation window.

4. Click **Yes**.

The network isolation rule for the host is deleted.

## Limitations that are relevant to network isolation

Some limitations apply when network isolation is used:

- When a network isolation rule is enabled on a host, all current connections are disconnected and a VPN connection becomes unavailable.
- If the program administrator replaces the certificate of the server with the Central Node component while a network isolation rule is enabled, you cannot disable the rule.
- 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.

# 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 (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.

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.

Users with the **Security officer** role do not have access to 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**—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.
   - **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 (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.

   This opens the task table.

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.
- **Run as**—Option to run the application using the name of the local system.
- **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.

   This opens the task table.

2. Click the **Add** button and select **Kill process**.

   This opens the task creation window.

3. Configure the following settings:

   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 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.

   This opens the task table.

2. Click the **Add** button and select **Run program**.

   This opens the task creation window.

3. Configure the following settings:

   a. In the **File path** and **Working directory** fields, enter values in one of the following ways:

   - In the **File path** field, enter the full path to the executable file (for example, `C:\Windows\System32\ipconfig.exe`). Leave the **Working directory** field empty.
   - In the **File path** field, enter the name and extension of the executable file (for example, `ipconfig.exe`). In the **Working directory** field, enter the path to the folder containing the executable file (for example, `C:\Windows\System32\`).

   b. In the **Arguments** field, enter additional options for running the file or task (for example, the `/all` argument).

   c. In the **Description** field, enter the task description. This field is optional.

   d. Configure the **Task for** setting, that is, the 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 run the `ipconfig /all` command on the host with IP address `10.10.10.1`:*

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click the **Add** button and select **Run program**.

   This opens the task creation window.

3. Configure the following settings:

   a. In the **File path** and **Working directory** fields, enter values in one of the following ways:

   - In the **File path** field, enter `C:\Windows\System32\ipconfig.exe`. Leave the **Working directory** field empty.
   - In the **File path** field, enter `ipconfig.exe`. In the **Working directory** field, enter `C:\Windows\System32\`.

   b. In the **Arguments** field, enter `/all`.

   c. In the **Description** field, enter the task description.

   d. Select the **Specified hosts** task scope.

   e. In the **Hosts** field, start entering characters of the IP address `10.10.10.1`, and when this IP address is displayed in the drop-down list of search results below, select it.

4. Click the **Add** button.

# Creating a file download task

The file to be downloaded must not exceed 100 MB. If the file exceeds 100 MB, the task does not proceed.

*To create a file download task:*

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click the **Add** button and select **Get file**.

   This opens the task creation window.

3. Configure the following settings:

   a. **File path**—Path to the file that you want to receive.

   If the requested file is linked to other NTFS data streams, running the task yields all files of NTFS data streams that the requested file is linked to.

   You can also specify the path to an alternate data stream of this file. In this case, you receive only the files of the specified stream.

   b. **MD5/SHA256**—MD5- or SHA256 hash of the file that you want to receive. 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. **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 Storage.

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.

   This opens the task table.

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 **Download**.

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.

   This opens the task table.

2. Click the **Add** button and select **Delete file**.

   This opens the task creation window.

3. Configure the following settings:

   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. **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 id not supported.

# Creating a file quarantine task

If you believe that an infected or probably infected file is on the computer with the Kaspersky Endpoint Agent program, you can isolate it by putting it into quarantine. The file is deleted from its folder on the computer and placed in Kaspersky Endpoint Agent quarantine on the same computer, in the quarantine directory that is configured in Kaspersky Endpoint Agent settings.

*To create a file quarantine task:*

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click the **Add** button and select **Quarantine file**.

   This opens the task creation window.

3. Configure the following settings:

   a. In the **File path** field, enter the path to the file that you want to put in quarantine.

   b. In the **MD5/SHA256** field, enter the MD5 or SHA256 hash of the file that you want to place in quarantine. This field is optional.

   c. In the **Description** field, enter the task description. This field is optional.

   d. In the **Hosts** field, type characters to search for the name of the host where the file you want to quarantine is located, and select the host name from the list. Repeat the steps for each host you want to add.

   Selected hosts are added to the list.

4. Click the **Add** button.

   The file quarantine task is created. As a result of the task:

   - The file is deleted from its folder on the computer with the Kaspersky Endpoint Agent program and placed in Kaspersky Endpoint Agent quarantine on the same workstation, in the quarantine directory that is configured in Kaspersky Endpoint Agent settings.
   - In the task list of the **Tasks** section of the program web interface, execution information about the task is displayed.
   - In the file list in the **Storage** section, **Quarantine** subsection, information about the quarantined file is displayed.

If the file has been blocked by another process, the task is displayed with the Completed status but the file is 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.

The file quarantine task can finish with the **Access denied** error if you are trying to quarantine an executable file and it is currently running.

To solve this problem, create a process termination task for this file, and then try creating the file quarantine task again.

# 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.

   This opens the task table.

2. Click the **Add** button and select **Restore file from Quarantine**.

   This opens the task creation window.

3. Configure the following settings:

   a. **Description**—Task description. This field is optional.

   b. **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.
   This opens the task table.
2. Open the task that you want to copy.
3. Click the **Duplicate** button.
   This opens the task creation window. All task settings will be copied.
4. If you want to modify task settings, edit one or more settings depending on the type of the task being copied.
5. Click the **Add** button.

A copy of the selected task will be created.

# Deleting tasks

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.
   This opens the task table.
2. Open the task that you want to delete.
3. Click **Delete**.
   This opens the action confirmation window.
4. Click **Yes**.

The task will be deleted.

*To delete all or multiple tasks:*

1. Select the **Tasks** section in the program web interface window.
   This opens the task table.

2. Select check boxes next to the tasks that you want to delete.

   You can select all tasks by selecting the check box in the row containing the headers of columns.

3. In the pane that appears in the lower part of the window, click **Delete**.

   This opens the action confirmation window.

4. Click **Yes**.

The selected tasks are 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.

   This opens the task table.

2. Click the **Time** 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 **Apply**.

   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.

   This opens the task table.

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.
   - **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 (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.

   This opens the task table.

2. Click the **Name** link to open the task filtering menu.

3. Select one or more check boxes:

   - **Kill process**.
   - **Run program**.
   - **Get file**.
   - **Delete file**.

- **Quarantine file**.
- **Restore file**.

4. Click **Apply**.

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.
   This opens the task table.
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 **Apply**.

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.

   This opens the task table.

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 **Apply**.

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.

   This opens the task table.

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.

   This opens the task table.
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 **Apply**.

   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.

   This opens the task table.
2. Click the **State** link to open the task filtering menu.

3. Select one or more check boxes:

   - **Pending**.
   - **In process**.
   - **Completed**.

4. Click **Apply**.

   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.

   This opens the task table.

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 manage prevention rules for files and processes on selected hosts. For example, you can prevent the running of programs that you consider unsafe to use on the selected host with Kaspersky Endpoint Agent. The program identifies files based on their hash by using the MD5 and SHA256 hashing algorithms. You can create, enable, disable, delete, and modify prevention rules. Additionally, you can click the link with the name of the hashing algorithm in the prevention rule table to find objects, events, or alerts that have triggered prevention rules, for example, **Find events**, **Find alerts**, **Find on KL TIP**, or **Find on virustotal.com**.

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.

Users with the **Senior security officer** role can create, edit, delete, enable and disable prevention rules for the organizations whose data they can access. 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.

Prevention rules can be created automatically based on preset politics (hereinafter also "presets") added by default. With presets turned on, a prevention rule is created based on a medium or high severity alert of the Sandbox component. The prevention rule thus created prevents running the file based on its MD5 hash. Users with the **Senior security officer** role can enable and disable presets.

Presets are not supported in distributed solution and multitenancy mode.

The same operations can be applied to automatically created prevention rules as for manually created rules.

You can create only one prevention rule for each file hash.

Prevention rules are enforced only when Kaspersky Endpoint Agent is running on the host.

If an attempt is made to run a file before Kaspersky Endpoint Agent is started or after Kaspersky Endpoint Agent is shut down on a host, the file is not blocked from running.

# 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.

   - **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** are names of servers with the PCN or SCN role to which the prevention rule applies.

   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 KL TIP.
   - **Find on virustotal.com** (for SHA256).
   - Find events.

     When this action is performed, the **Threat Hunting** section opens with events that are already filtered based on the hash you selected.

   - Find alerts.

     When this action is performed, the **Alerts** section opens with alerts 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**
   - **Limited functionality**

# Viewing a prevention rule

*To view information about a prevention rule:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

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**
  - **Limited functionality**
- The **Details** tab contains the following information:
  - **MD5/SHA256** is the hash of the file prevented from running.

    Clicking the **MD5/SHA256** link opens a list in which you can select one of the following actions:

    - **Find on KL TIP**
    - **Find events**.
    - **Find alerts**.
    - **Copy value to clipboard**.
  - **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.
    - **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.

   This opens the prevention rule table

2. Click the **Add** button.

   This opens the prevention rule creation window.

3. Configure the following settings:

   a. **State** is the state of the prevention rule:

   - If you want to enable the prevention rule, set the toggle switch to **On**.
   - If you want to disable the prevention rule, set the toggle switch to **Off**.

   b. **MD5/SHA256**—MD5- or SHA256 hash of the file or data stream that you want to prevent from starting.

   c. **Name** is the name of the prevention rule.

   d. 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.

   e. **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 rule

*To enable or disable a prevention rule:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

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 **Limited functionality**.

     The prevention rule you selected will be disabled.

# Enabling and disabling presets

*To enable or disable presets:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

2. Select the **Presets** tab.

3. In the row of the preset that you want to enable or disable, in the **State** column, set the toggle switch to **Enabled** or **Limited functionality**.

The preset is enabled or disabled. When a preset is disabled, all prevention rules that were previously automatically created are not removed.

# Deleting prevention rules

You can delete a single prevention rule or multiple prevention rules, or all prevention rules at the same time.

*To delete a prevention rule:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

2. Click the prevention rule that you want to delete.

   This opens the prevention rule details window.

3. Click **Delete**.

   This opens the action confirmation window.

4. Click **Yes**.

The prevention rule will be deleted.

*To delete all or multiple prevention rules:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

2. Select check boxes next to prevention rules that you want to delete.

   You can select all prevention 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**.

   This opens the action confirmation window.

4. Click **Yes**.

The selected prevention rules are deleted.

# Filtering prevention rules by name

*To filter prevention rules by name:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

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 text box, enter one or more characters of the prevention rule name.

5. To add a filter condition using a different criterion, click + and specify the filter condition.

6. Click **Apply**.

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.

   This opens the prevention rule table

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.
   - **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 prevention rules by file hash

*To filter prevention rules by file hash:*

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table

2. Click the **File hash** link to open the prevention rule 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 **Apply**.

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 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.

   This opens the prevention rule table
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 **Apply**.

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.

   This opens the prevention rule table
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 user-defined rules

Users with **Security officer** or **Senior security officer** roles can manage **TAA**, **IDS**, **IOC**, and **YARA** user rules: upload and delete rule files, view tables of uploaded rules in the **User rules** section, and manage **IDS** and **TAA** rule that are added to exclusions in the **Program settings** section, **White lists** subsection of the program web interface.

# Using indicators of compromise (IOC) and attack (IOA) for Threat Hunting

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 a "TAA (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 Events database of the program and marks events that match behaviors described by TAA (IOA) rules. The *streaming scan* technology is used, which involves continuous real-time scanning of objects downloaded from the network.

TAA (IOA) rules created by Kaspersky experts are used by the TAA (Targeted Attack Analyzer) technology and are updated alongside the program databases. They are not displayed in the interface of the program and cannot be edited.

You can add user-defined IOC and TAA (IOA) rules using IOC files in the OpenIOC format as well as create TAA (IOA) rules based on event database search conditions.

The following table contains a comparative analysis of indicators of compromise (IOC) and attack (IOA).

Comparison of IOC and IOA indicators

| Characteristic | IOC in user-defined IOC rules | IOA in user-defined TAA (IOA) rules | IOA in TAA (IOA) rules created by Kaspersky experts |
|---|---|---|---|
| Scan scope | Computers with Kaspersky Endpoint Agent | Program events database | Program events database |
| Scanning mechanism | Periodical scan | Streaming scan | Streaming scan |
| Can be added to exclusions from scan | None. | Not needed.<br>Users with the **Senior security officer** role can edit the text of the indicator in custom TAA (IOA) rules as necessary. | Yes. |

If you are using the distributed solution and multitenancy mode, the section displays data on the organization that you chose.

# Managing user-defined IOC rules

You can use IOC files to search indicators of compromise on hosts with Kaspersky Endpoint Agent installed.

Users with the **Senior security officer** role can upload, delete, download IOC files to their computer, enable or disable the search of indicators of compromise using IOC files, as well as configure the schedule for searching indicators of compromise on hosts with Kaspersky Endpoint Agent program installed.

Users with the **Security officer** role can view the list of IOC files and information about the selected file, and download IOC files to the computer.

IOC files can have the following types:

- **Global**—IOC files uploaded to the PCN server. These IOC files are used to search for indicators of compromise on Kaspersky Endpoint Agent hosts connected to the PCN server and all SCN servers connected to the PCN server.
- **Local**—IOC files uploaded to an SCN server. These IOC files are used to search for indicators of compromise on Kaspersky Endpoint Agent hosts connected to the SCN server.

To view the list of supported OpenIOC indicators of compromise, you can download this file.

## Viewing the table of IOC files

The table of IOC files contains information about IOC files used for scanning on hosts with the Kaspersky Endpoint Agent program installed; you can find the table in the **User rules** section, **IOC** 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**—IOC files uploaded to the PCN server. These IOC files are used to search for indicators of compromise on Kaspersky Endpoint Agent hosts connected to the PCN server and all SCN servers connected to the PCN server.
   - **Local**—IOC files uploaded to an SCN server. These IOC files are used to search for indicators of compromise on Kaspersky Endpoint Agent hosts connected to the SCN server.

3. **Name**—Name of the IOC file.

4. **Servers**—Name of the server with the Central Node component.

5. **Autoscan**—The IOC file is used when automatically scanning Kaspersky Endpoint Agent hosts:

   Host scanning using this IOC file can have one of the following statuses:

   - **Enabled**
   - **Limited functionality**

## Viewing information about an IOC file

*To view information about an IOC file:*

1. In the window of the program web interface, select the **User rules** section, **IOC** subsection.

   This opens the table of IOC files.

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:

- Clicking the **Find alerts** link opens the **Alerts** section with the filter condition populated with the name of your selected IOC file.
- Clicking the **Find events** link opens the **Threat Hunting** section with the search condition populated with indicators of compromise of your selected IOC file.
- Clicking the **Download file** link opens the IOC file download window.
- **Autoscan**—The IOC file is used when automatically scanning Kaspersky Endpoint Agent hosts.

  Host scanning using this IOC file can have one of the following statuses:

  - **Enabled**
  - **Limited functionality**
- **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 window of the program web interface, select the **User rules** section, **IOC** subsection.
2. This opens the IOC file table. Click **Upload**.

   This opens the file selection window on your local computer.
3. Select the file that you want to upload and click **Open**.
4. Specify the following parameters:

   a. **Autoscan**—Use of an IOC file during an automatic scan of events:

   - **Enabled**
   - **Limited functionality**

   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 **Save**.

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 window of the program web interface, select the **User rules** section, **IOC** subsection.
2. This opens the IOC file table. 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 for searching for indicators of compromise on Kaspersky Endpoint Agent hosts.

*To enable or disable the automatic use of an IOC file for searching for indicators of compromise on Kaspersky Endpoint Agent hosts:*

1. In the window of the program web interface, select the **User rules** section, **IOC** subsection.

   This opens the table of IOC files.
2. In the line containing the IOC file whose use you want to enable or disable, in the **State** column, set the toggle switch to one of the following positions:

   - **Enabled**
   - **Limited functionality**

Automatic use of an IOC file for searching for indicators of compromise on Kaspersky Endpoint Agent hosts is enabled or disabled.

Users with the **Security officer** role cannot enable or disable automatic application of a IOC file when scanning events.

## Deleting an IOC file

*To delete an IOC file:*

1. In the window of the program web interface, select the **User rules** section, **IOC** subsection.

   This opens the table of IOC files.

2. Select the IOC file that you want to delete.
   This opens a window containing information about the IOC file.
3. Click **Delete**.

The IOC file will be deleted.

Users with the **Security officer** role cannot delete IOC files.

## Searching for alerts in IOC scan results

*To find and view scan results for the selected IOC file:*

1. In the window of the program web interface, select the **User rules** section, **IOC** subsection.
   This opens the table of IOC files.
2. Select the IOC file for which you want to view scan results.
   This opens a window containing information about the IOC file.
3. Go to the alert database by clicking **Find alerts**.
   The alert table is opened in a new browser tab.

You can also view scan results for all IOC files by filtering alerts by technology name.

## Searching for alerts using an IOC file

*To view the events that were found using an IOC file:*

1. In the window of the program web interface, select the **User rules** section, **IOC** subsection.
   This opens the table of IOC files.
2. Select the IOC file to use for searching for events in the event database.
   This opens a window containing information about the IOC file.
3. Go to the event database by clicking **Find events**.
   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 window of the program web interface, select the **User rules** section, **IOC** subsection.
2. This opens the IOC file table. Do the following depending on the filtering criterion:

- **By importance**

  a. Click the icon to open the filter configuration window for IOC files.

  b. Select one or several of the following importance levels:

  - **Low**.
  - **Medium**.
  - **High**.

  c. Click **Apply**.

- **By file name**

  a. Click the **Name** link to open the IOC file filter configuration window.

  b. Enter one or several characters of the IOC file name.

  c. Click **Apply**.

- **By the state of the automatic scan (enabled / disabled)**

  a. Click the **Autoscan** link to open the filter configuration window for IOC files.

  b. Select one of the following options:

  - **Enabled**
  - **Limited functionality**

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 window of the program web interface, select the **User rules** section, **IOC** subsection.
2. This opens the IOC file table. Click to the right of the header of the IOC file table column for which you want to clear the filtering 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 the schedule for searching for indicators of compromise using IOC files on Kaspersky Endpoint Agent hosts.

*To configure the schedule for searching for indicators of compromise using IOC files on Kaspersky Endpoint Agent hosts:*

1. In the window of the program web interface, select the **Program settings** section, **IOC scanning schedule** subsection.
2. In the **Start time** drop-down lists, select the start time of the indicator of compromise search.
3. In the **Maximum scan duration** drop-down list, select a time limit for completing the indicator of compromise search.
4. Click **Save**.

The new schedule for searching for indicators of compromise using IOC files on Kaspersky Endpoint Agent hosts becomes active immediately after changes are saved. Results of the indicator of compromise search are displayed in the alert table.

Users with **Security officer** role cannot configure the schedule for searching for indicators of compromise using IOC files on Kaspersky Endpoint Agent hosts.

# Managing user-defined TAA (IOA) rules

Users with the **Senior security officer** role can create, import, delete, enable or disable TAA (IOA) rules, and exclude Kaspersky TAA (IOA) rules from scanning. Users with the **Senior security officer** or **Security officer** roles can use TAA (IOA) rules to search for signs of targeted attacks, infected and possibly infected objects in the database of events and alerts, and to view the TAA (IOA) rule table and TAA (IOA) rule information.

The differences between user rules and Kaspersky rules are summarized in the following table.

Comparison of TAA (IOA) rules

| Characteristic | User-defined TAA (IOA) rules | Kaspersky TAA (IOA) rules |
|---|---|---|
| Recommendations on responding to the event | No | Yes<br>You can view recommendations in alert information |
| Correspondence to technique in MITRE ATT&CK database | No | Yes<br>You can view the description of the technique according to the MITRE database in alert information |
| Display in the в TAA (IOA) rule table | Yes | No |
| Ability to disable database lookup for this rule | Disable rule | Add rule to white list |
| Ability to delete or add the rule | You can delete or add a rule in the web interface of the program | Rules are updated together with program databases and cannot be deleted by the user |
| Searching for alerts and events in which TAA (IOA) rules were triggered | Using **Alerts** and **Events** links in the TAA (IOA) rule information window | Using **Alerts** and **Events** links in the alert information window |

Depending on the program operating mode and the server on which the TAA (IOA) rules are created, user-defined TAA (IOA) rules can have one of the following types:

- **Local**—Created on the SCN server. These 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 (in the distributed solution and multitenancy mode).
- **Global**—Created on the PCN server. These 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 (in the distributed solution and multitenancy mode).

## Viewing the TAA (IOA) rule table

The table of user-defined TAA (IOA) rules contains information about TAA (IOA) rules that are used to scan events and create alerts; the table is in the **User rules** section, **TAA** subsection of the program web interface window.

The table contains the following information:

1. —Importance level that is assigned to an alert generated using this TAA (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 which generated it in distributed solution 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 Targeted Attack Analyzer (TAA) technology specified.
   - **Limited functionality** – not displayed in the alert table.
7. **State** – usage status of the rule in event scans:
   - **Enabled** – the rule is being used.
   - **Limited functionality** – the rule is not being used.

## Viewing the information of a user-defined TAA (IOA) rule

*To view information about a TAA (IOA) rule:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.

   This opens the TAA (IOA) rule table.
2. Select the rule for which you want to view information.

This opens a window containing information about the rule.

The window contains the following information:

- **Alerts**. Click the link to display the **Alerts** table in a new browser tab. The alerts are filtered by the **Technologies** and **Details** columns, that is, the Targeted Attack Analyzer technology and the name of the TAA (IOA) rule that you are working on.
- **Find events**. Click the link to display the **Threat Hunting event table** in a new browser tab. The table is filtered by rule name.

- **Run query**. Click the link to display the **Threat Hunting event table** in a new browser tab. The table is filtered by rule name. The event search conditions are populated with information from the TAA (IOA) rule that you are working on. For example, `EventType=Process started AND FileName CONTAINS <name of the rule you are working on>`. You can edit the event search query.

- **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 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 (in the distributed solution and multitenancy mode).

  - **Local**—Created on the SCN server. These 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 (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. Click the **Run query** link in the upper part of the window to go to the **Threat Hunting** section and run an event search query.

## Searching for alerts and events in which TAA (IOA) rules were triggered

*To search and display alerts and events that were created by a user-defined TAA (IOA) rule triggering:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.

   This opens the TAA (IOA) rule table.

2. Select the rule for which you want to view the triggering result.

   This opens a window containing information about the rule.

3. Do one of the following:

   - If you want to view alerts generated by the TAA (IOA) rule triggering, click **Alerts** to go to the alerts database.

     The alert table is opened in a new browser tab.

- If you want to view events generated by the TAA (IOA) rule triggering, click **Events** to go to the events database.

  The event table is opened in a new browser tab.

*To search and display alerts and events that were created by a Kaspersky TAA (IOA) rule triggering:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

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 the **(TAA) Targeted Attack Analyzer** technology.

5. Click **Apply**.

   The table displays alerts generated by the TAA technology based on TAA (IOA) rules.

6. Select an alert for which the **Detected** column displays the name of the relevant 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 TAA (IOA) rule triggering, click **Alerts** to go to the alerts database.

     The alert table is opened in a new browser tab.

   - If you want to view events generated by the TAA (IOA) rule triggering, click **Events** to go to the events database.

     The event table is opened in a new browser tab.

## Filtering and searching TAA (IOA) rules

*To filter or search for TAA (IOA) files based on required criteria:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.

   This opens the TAA (IOA) rule table.

2. Depending on the filtering criterion, do the following:

- **By importance**

  a. Click the icon to open the IOA rule filter configuration window.

  b. Select the check boxes next to the importance levels that you want to include in the filter criteria:

  - **Low**.
  - **Medium**.
  - **High**.

  c. Click **Apply**.

- **By rule type**

  a. Click the **Type** link to open the filter configuration window.

  b. Select one of the following options:

  - **All** – all rules.
  - **Global** – rules created on the PCN server. These 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 (in the distributed solution and multitenancy mode).
  - **Local** – rules create on an SCN server. These 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 (in the distributed solution and multitenancy mode).

- **By confidence level**

  a. Click the **Confidence** link to open the filter configuration window.

  b. Select the check boxes opposite those confidence levels that you want to add to filter criteria.

  - **Low**.
  - **Medium**.
  - **High**.

  c. Click **Apply**.

- **By rule name**

  a. Click the **IOA tag** link to open the filter configuration window.

  b. Enter one or several characters of the IOA rule name.

  c. Click **Apply**.

- **By server name**

  a. Click the **Servers** link to open the filter configuration window.

  b. Select the check boxes next to the organizations or servers within the organizations that you want to include in the filter criteria.

  c. Click **Apply**.

- **By rule-based alert generation**

  a. Click the **Generate alerts** link to expand the filter settings list.

  b. Select one of the following options:

  - **All**
  - **Enabled**
  - **Limited functionality**

- **By rule state**

  a. Click **State** to expand the filter settings list.

  b. Select one of the following options:

  - **All**
  - **Enabled**
  - **Limited functionality**

The table displays only rules that match the specified criteria.

You can use multiple filters at the same time.

## Resetting the TAA (IOA) rule filter

*To clear a TAA (IOA) rule filter based on one or multiple filter conditions:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.
   This opens the TAA (IOA) rule table.
2. Click on the right of the templates table column heading 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 displays only rules that match the specified criteria.

## Creating a user-defined TAA (IOA) rule based on event search conditions

*To create a user-defined TAA (IOA) based on event search conditions:*

1. Select the **Threat Hunting** section in the program web interface window.

   This opens the event search form.

2. Perform an event search in design mode or source code mode.

3. Click the **Save as TAA (IOA) rule** button.

   This opens the **New TAA (IOA) rule** window.

4. In the **Name** field, type the name of the rule.

5. Click **Save**.

   The event search condition will be saved. In the TAA (IOA) rule table in the **User rules** section, **TAA** subsection of the web interface, the new rule is displayed with the specified name.

If you want to save event search conditions as a user-defined TAA (IOA) rule, avoid using the following fields:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

At the time of saving the user-defined TAA (IOA) rule, the program might not have any events containing data for these fields. When events with this data turn up, the user-defined field that you have created earlier will be unable to mark events by these fields.

## Importing a user-defined TAA (IOA) rule

You can import an IOC format file and use it to scan events and create Targeted Attack Analyzer alerts.

It is highly recommended to test custom TAA (IOA) rules in a test environment before you import them. Custom TAA (IOA) rules may cause performance issues, in case of which stable performance of Kaspersky Anti Targeted Attack Platform is not guaranteed

*To import a TAA (IOA) rule:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.

   This opens the TAA (IOA) rule table.

2. Click **Import**.

   This opens the file selection window on your local computer.

3. Select the file that you want to upload and click **Open**.

   This opens the **New TAA (IOA) rule** window.

4. Select or clear the **State** check box if you want to change the usage status of the rule when scanning the events database.

5. On the **Details** tab, 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 TAA (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 **Save**.

The user-defined TAA (IOA) rule is imported into the program.

You can also add a TAA (IOA) rule by saving events database search conditions in the **Threat Hunting** section.

## Enabling and disabling TAA (IOA) rules

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 a TAA (IOA) rule when scanning events:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.
   This opens the TAA (IOA) rule table.
2. In the row with the relevant rule, select or clear the check box in the **State** column.

The use of the rule when scanning events is enabled or disabled.

*To enable or disable the use of all or multiple TAA (IOA) rules when scanning events:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.
   This opens the TAA (IOA) rule table.
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.

The use of the selected rules when scanning events is enabled or disabled.

These changes do not affect TAA (IOA) rules defined by Kaspersky. If you do not want to use a Kaspersky TAA (IOA) rule for scanning, add it to exclusions.

## Modifying a user-defined TAA (IOA) rule

You can edit only user-defined TAA (IOA) rules. Rules created by Kaspersky cannot be edited.

When working in distributed solution and multitenancy mode, you can edit only those TAA (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 change a TAA (IOA) rule:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.
   This opens the TAA (IOA) rule table.
2. Select the rule that you want to modify.
   This opens a window containing information about the rule.
3. Make the relevant changes.
4. Click **Save**.

The rule settings are modified.

# Deleting user-defined TAA (IOA) rules

You can delete a single TAA (IOA) rule, multiple rules, or all rules.

When working in distributed solution mode, you can delete only those TAA (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 a user-defined TAA (IOA) rule:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.

   This opens the TAA (IOA) rule table.

2. Select the rule that you want to delete.

   This opens a window containing information about the rule.

3. Click **Delete**.

   This opens the action confirmation window.

4. Click **Yes**.

The rule is deleted.

*To delete all or multiple TAA (IOA) rules:*

1. In the window of the program web interface, select the **User rules** section, **TAA** subsection.

   This opens the TAA (IOA) rule table.

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 **Delete**.

   This opens the action confirmation window.

4. Click **Yes**.

The selected rules will be deleted.

You cannot delete TAA (IOA) rules defined by Kaspersky. If you do not want to use a Kaspersky TAA (IOA) rule for scanning, add it to exclusions.

# Managing user-defined IDS rules

Users with the **Senior security officer** role can import, configure, replace, and delete user-defined IDS rules, as well as add Kaspersky-defined IDS rules to exclusions from scanning. Users with the **Senior security officer** or **Security officer** roles can use IDS rules to search for signs of targeted attacks, infected and possibly infected objects in the alert database, and to view the IDS rule information.

Depending on the program operating mode and the server on which the IDS rules are created, user-defined IDS rules can have one of the following types:

- **Local**—Created on the SCN server. These 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 (in the distributed solution and multitenancy mode).
- **Global**—Created on the PCN server. These 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 (in the distributed solution and multitenancy mode).

## Importing a user-defined IDS rule

You can import a Snort® or Suricata file and use it to scan events and create Intrusion Detection System alerts.

It is highly recommended to test custom IDS rules in a test environment before you import them. Custom IDS rules may cause performance issues, in which case stable performance of Kaspersky Anti Targeted Attack Platform is not guaranteed

For example, loading user-defined rules can cause the following errors:

- The application may create too many IDS alerts.
- If the application cannot log all IDS alerts in time, some network traffic objects may remain unscanned.
- Regular expressions in user-defined rules may impact performance or cause faulty operation of the application.
- Even formally correct user-defined rules may impact performance or cause faulty operation of the application.

IDs and attributes of custom rules may be modified when uploaded. Reject and Drop actions will be changed to Alert. Rules with the Pass action will be deleted

*To import a user-defined IDS rule:*

1. In the window of the program web interface, select the **User rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window. Click **Import**.
   This opens the file selection window on your local computer.
3. Select the file that you want to upload and click **Open**.

The user-defined IDS rule is imported into the program.

## Viewing the information of a user-defined IDS rule

*To view the information of a user-defined IDS rule,*

in the window of the program web interface, select the **User rules** section, **IDS** subsection.

The web interface displays the following information about the IDS rule:

- **State**—Usage status of the rule in event scans.
- **File size**—Size of the rule file.
- **Last update**—Time when the rule was imported.
- **Created by**—Name of the user whose account was used to import the rule.
- **Importance**—Importance level that is assigned to an alert generated using this IDS rule.

## Enabling and disabling the use of an IDS rule when scanning events

*To enable or disable the use of an IDS rule when scanning events:*

1. In the window of the program web interface, select the **User rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window. Move the **State** switch to one of the following positions:
   - **Enabled**
   - **Limited functionality**

The use of the IDS rule when scanning events is enabled or disabled.

## Configuring the importance of alerts generated by the user-defined IDS rule

*To configure the importance level that is assigned to alerts generated using the IDS rule:*

1. In the window of the program web interface, select the **User rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window. In the **Importance** drop-down list, select the importance level to be assigned to alerts generated using this IDS rule.
   - **Low**.
   - **Medium**.
   - **High**.
3. If you want to enable the use of this IDS rule for event scanning, turn on the **State** switch.

The importance of alerts generated using this IDS rule is configured.

## Replacing a user-defined IDS rule

You can replace a previously imported Snort or Suricata file and use it to scan events and create Intrusion Detection System alerts.

It is highly recommended to test custom IDS rules in a test environment before you import them. Custom IDS rules may cause performance issues, in which case stable performance of Kaspersky Anti Targeted Attack Platform is not guaranteed

IDs and attributes of custom rules may be modified when uploaded. Reject and Drop actions will be changed to Alert. Rules with the Pass action will be deleted

*To replace a user-defined IDS rule:*

1. In the window of the program web interface, select the **User rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window. Below the rule information, click **Replace**.

   This opens the file selection window on your local computer.
3. Select the file that you want to upload and click **Open**.

The user-defined IDS rule is imported into the program, replacing the previously imported rule.

## Downloading a user-defined IDS rule file to the computer

You can download a previously imported IDS rule file to your computer.

*To download a user-defined IDS rule file to your computer:*

1. In the window of the program web interface, select the **User rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window. Below the rule information, click **Download**.

   The file will be saved to your local computer in the browser's downloads folder.

## Deleting a user-defined IDS rule

When working in distributed solution mode, you can delete only those user-defined IDS rules that were imported into the current server. It means that in the PCN web interface, you can only delete a rule that was created on the PCN. In the SCN web interface, you can only delete a rule that was created on the SCN.

*To delete a user-defined IDS rule:*

1. In the window of the program web interface, select the **User rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window. Click **Delete**.

   This opens the action confirmation window.
3. Click **Yes**.

   The rule is deleted.

You cannot delete IDS rules defined by Kaspersky. If you do not want to use a Kaspersky IDS rule for scanning, add it to exclusions.

# Managing YARA rules

YARA rule files are used as databases of the YARA module.

You can create your own YARA rules and add a YARA rule file to Kaspersky Anti Targeted Attack Platform using the program web interface.

For more information about creating and updating YARA rules of version 3.7.0 and higher, refer to the documentation on YARA rules.

## Uploading YARA rules

*To upload YARA rules:*

1. In the window of the program web interface, select the **User rules** section, **YARA** subsection.
2. Click **Upload**.
   This opens the file selection window.
3. Select the YARA rules file that you want to upload and click the **Open** button.
   This closes the file selection window.

The following information about the uploaded YARA rules is displayed:

- **File size**—Size of the 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 **User rules** section, **YARA** subsection.
2. Click the **Replace** button.
   This opens the file selection window.
3. Select the YARA rules file that you want to replace the current file with and click **Open**.
   This closes the file selection window.

The uploaded YARA rules file replaces the previous file.

## Deleting YARA rules

*To delete YARA rules:*

1. In the window of the program web interface, select the **User rules** section, **YARA** subsection.
2. Click **Delete**.
   This opens the action confirmation window.
3. Click **Yes**.

YARA rules are deleted.

# Managing objects in Storage and Quarantine

You can place copies of objects that you want to scan into special Storage.

Storage is located on the Central Node server.

You can manage objects in Storage 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 Storage as a table of objects.

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 Storage of all connected SCNs for organizations, which the user is allowed to access.

Users with the **Senior security officer** role can place copies of objects into Storage using the **Get file** task or by manually uploading the object to Storage on the PCN or SCN server which is used to manage organizations that the user is allowed to access.

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.

If you consider a file threatening, you can quarantine it on the computer with the Kaspersky Endpoint Agent program. Metadata of the quarantined file are displayed in the **Storage** section, **Quarantine** subsection of the Kaspersky Anti Targeted Attack Platform web interface.

*Quarantine on Kaspersky Endpoint Agent hosts* – is a special local storage for files that you consider unsafe. Quarantined files are stored in encrypted form and do not threaten the security of the computer.

When a file is quarantined on a Kaspersky Endpoint Agent host, it is moved rather than copied: the object is deleted from the directory where it was detected and placed in the quarantine directory that is specified in Kaspersky Endpoint Agent settings.

*Quarantine on a Kaspersky Anti Targeted Attack Platform* server is an area of Storage of the server part of the Kaspersky Anti Targeted Attack Platform solution, which is used for storing metadata of objects quarantined on Kaspersky Endpoint Agent computer, in the **Storage** section, **Quarantine** subsection of the web interface of Kaspersky Anti Targeted Attack Platform.

You can manage quarantined objects: restore objects from quarantine and upload copies of objects quarantined on Kaspersky Endpoint Agent computers to Storage of Kaspersky Anti Targeted Attack Platform.

Kaspersky Anti Targeted Attack Platform displays the information about quarantined objects as a table.

The default maximum Storage space is 10 GB. As soon as this threshold value is exceeded, the program starts to remove the oldest copies of objects from Storage. When the amount of occupied space is again below the threshold value, the program stops removing copies of objects from Storage.

The actual size of the object can be greater than the apparent size of the object due to the metadata required to restore the object from Quarantine. When an object is quarantined, its 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 Storage

The table of objects placed in Storage is in the **Storage** section, **Files** subsection of the program web interface window.

The table of objects placed in Storage contains the following information:

1. **Type**—Location of the object in Storage.

   The following types of objects are available:

   - – The object was placed in Storage in one of the following ways:
     - A **Quarantine file** task was run in the **Tasks** section.
     - A **Get file** task was run in the **Tasks** section.
     - A copy was received of an object that was quarantined on hosts with Kaspersky Endpoint Agent (in the **Storage** section, **Quarantine** subsection, **Get file from Quarantine** action was selected in the menu for the link with the directory of the object).
   - – The object was manually downloaded by the user in the **Storage** section, **Files** subsection.

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. A host from which the object was received is connected to this server (displayed if you are using the distributed solution and multitenancy mode).

5. **Update 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 Storage.

The right part of the object information row contains buttons:

- You can click to delete the object from Storage.
- You can click to send the object in Storage for scanning by the Anti-Malware Engine, YARA, and Sandbox technologies.
- You can click to download the object from Storage to your computer.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Filter by this value**.
- **Exclude from filter**.
- **Download file**.
- **Send file for scanning**.
- Find events:
  - **File path**.
  - **MD5**.
  - **SHA256**.
- Find alerts:
  - **File path**.
  - **MD5**.
  - **SHA256**.
- **Copy value to clipboard**.

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**.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

# Viewing information about an object manually placed in Storage

*To view information about an object manually placed in Storage:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. In the table, select the object with the ↑ icon for which you want to view information.

   This opens the object details window.

The window contains the following information:

- **File name**—Name of the file.
- **Size**—Size of the file.
- **MD5**—MD5 hash of a file.
- **SHA256**—SHA256 hash of a file.
- **Time uploaded**—Time of upload for objects that were manually uploaded by a user.
- **User name**—Name of the user account that manually uploaded the object to Storage.
- **Scan results**—Result of object scan by the program.

The **Find on KL TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

Click **Create a prevention rule** to prevent the file from running.

You can click **Download** to download the file to your computer's hard drive.

Clicking the link with the file name opens a list in which you can select one of the following actions:

- **Find events**.
- **Find alerts**.
- **Copy value to clipboard**.

Clicking the link with **MD5** opens a list in which you can select one of the following actions:

- **Find on KL TIP**.
- **Find events**.
- **Find alerts**.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the link with **SHA256** opens a list in which you can select one of the following actions:

- Find on KL TIP.
- **Find on virustotal.com**.
- Find events.
- Find alerts.
- Create a prevention rule.
- **Copy value to clipboard**.

# Viewing information about an object placed in Storage by a task

*To view information about an object placed in Storage by a task:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. In the table, select the object with the icon for which you want to view information.

   This opens the object details window.

The window contains the following information:

- Recommendations group. The following recommendations can be displayed:
  - The Task link opens the **Tasks** section; this is the task that has placed the object in Storage.
  - The Alert link opens the **Alerts** section; this is the alert containing the object that was placed in Storage.
  - The **Quarantined object** link opens the **Storage** section, **Quarantine** subsection; this is the metadata of the quarantined object.
- **Object**—File name or path.
- **Size**—Size of the file.
- **MD5**—MD5 hash of a file.
- **SHA256**—SHA256 hash of a file.
- **Time stored**—Time when the object was placed in Storage.
- **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.
- **Scan results**—Result of object scan by the program.

You can click **Sandbox detect** to open a window with detailed information about the results of file behavior analysis.

The **Find on KL TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

Click **Create a prevention rule** to prevent the file from running.

You can click **Download** to download the file to your computer's hard drive.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Find events**.
- **Find alerts**.
- **Copy value to clipboard**.

Clicking the link with **MD5** opens a list in which you can select one of the following actions:

- **Find on KL TIP**.
- **Find events**.
- **Find alerts**.
- **Create a prevention rule**.
- **Copy value to clipboard**.

Clicking the link with **SHA256** opens a list in which you can select one of the following actions:

- **Find on KL TIP**.
- **Find on virustotal.com**.
- **Find events**.
- **Find alerts**.
- **Create a prevention rule**.
- **Copy value to clipboard**.

# Downloading objects from Storage

If you consider an object in Storage 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 Storage:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. In the right part of the row 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 Storage

If you need to scan a specific object, you can upload this object to Storage and send it to be scanned.

*To upload an object to Storage:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. In the upper right corner of the window, click **Upload**.

   This opens the file selection window.
3. Select the object that you want to upload to Storage, and click the **Open** button.

The object will be uploaded to Storage and will be displayed in the table of objects.

# Sending objects in Storage for scanning

You can scan Storage 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 Storage to be scanned in the following cases:

- Scanning of objects when placed in Storage had been disabled.
- Program databases have been updated.
- An object was manually uploaded to Storage.

*To send an object from Storage to be scanned:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click the object that you want to scan.

   This opens the object details window.
3. Click **Scan**.

The object scan will start.

After the object scan is complete, its status will be displayed in the object table.

You can also send an object in Storage for scanning by clicking in the right part of the object information row in the table of objects placed in Storage.

# Deleting objects from Storage

*To delete an object from Storage:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click the object that you want to delete.

   This opens the object details window.
3. Click **Delete**.

   This opens the action confirmation window.
4. Click **Yes**.

The object will be deleted from Storage.

You can also delete an object in Storage by clicking in the right part of the object information row in the table of objects placed in Storage.

*To delete all or multiple objects in Storage:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Select check boxes next to objects that you want to delete from Storage.

   You can select all objects by selecting the check box in the row containing the headers of columns.
3. In the pane that appears in the lower part of the window, click **Delete**.

   This opens the action confirmation window.
4. Click **Yes**.

The selected objects are removed from Storage.

# Filtering objects in Storage by object type

*To filter objects in Storage by type:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click the **Type** link to open the object filtering menu.

3. Select one or more check boxes:

   - **File placed in Storage by a task** if you want the table to display objects that have been placed in Storage by a task.
   - **File uploaded manually**, if you want the table to display objects that were manually uploaded by the user.

4. Click **Apply**.

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 Storage by object description

*To filter objects in Storage based on the object description:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. 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 **Apply**.

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 Storage based on scan results

*To filter objects in Storage based on the scan results for these objects:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click the **Scan results** link to open the object filtering menu.
3. Select one or more check boxes:
   - **Not detected**
   - **Error**
   - **In process**
   - **Not scanned**
   - **Detected**
4. Click **Apply**.

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 Storage based on the name of Central Node, PCN, or SCN server

*To filter objects in Storage 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.
2. This opens the object table. 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 Storage.
4. Click **Apply**.

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 Storage by object source

*To filter objects in Storage based on the source from which they were received:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click the **Update 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 **Apply**.

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 Storage

*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.
2. This opens the object table. 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 Storage.
   - **Last hour**, if you want the table to display objects that were placed in Storage during the last hour.

- **Last day**, if you want the table to display objects that were placed in Storage during the last day.
- **Custom range**, if you want the table to display objects that were placed in Storage 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 **Apply**.

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 Storage objects filter

*To clear a Storage objects filter based on one or multiple filter conditions:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click  to the right of the header of the Storage objects table column for which you want to clear the filtering 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 the table of objects quarantined on computers with Kaspersky Endpoint Agent

The table of objects quarantined on computers with the Kaspersky Endpoint Agent program can be found in the **Storage** section, **Quarantine** subsection of the application web interface.

The Kaspersky Anti Targeted Attack Platform server stores metadata of objects quarantined on computers with the Kaspersky Endpoint Agent program. The objects themselves are kept in special storage on each computer where the threatening object was detected.

The table of objects quarantined on computers with the Kaspersky Endpoint Agent program contains the following information:

1. **Object**—Information about the object. For example, the file name or file path.
2. **Update source**—IP address or host name of the computers with the Kaspersky Endpoint Agent program where the object is quarantined.
3. **Time stored**—Date and time when the object was quarantined.
4. **State**—State of the object.

The right part of the object information row contains buttons:

- You can click to delete the metadata of the object on the Kaspersky Anti Targeted Attack Platform server.
- You can click to restore the object from Quarantine on a computer the Kaspersky Endpoint Agent program.
- You can click to copy the object from Quarantine on the computer with the Kaspersky Endpoint Agent program to the Kaspersky Anti Targeted Attack Platform server.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- **Filter by this value**.
- **Exclude from filter**.
- **Download file**.
- **Send file for scanning**.
- Find events:
  - **File path**.
  - **MD5**.
  - **SHA256**.
- Find alerts:
  - **File path**.
  - **MD5**.
  - **SHA256**.
- **Copy value to clipboard**.

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**.

- Find events.
- Find alerts.
- **Copy value to clipboard**.

## Viewing information about a quarantined object

*To view information about an object quarantined on a computer with the Kaspersky Endpoint Agent program:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. In the table, select the object whose information you want to view.

   This opens the object details window.

The window contains the following information:

- Recommendations group. The **Task** recommendation can be displayed, which is a link that opens the **Tasks** section; this is the task that has quarantined the object.
- **Object**—File name or path.
- **Size**—Size of the file.
- **Time quarantined**—Date and time when the object was quarantined.
- **Company** —Name of the organization to which the Central Node, PCN, or SCN server belongs.
- **Host**—Name of the host with the Kaspersky Endpoint Agent program on which the object is quarantined.
- **File**—State of the file (whether a copy was obtained on the Kaspersky Anti Targeted Attack Platform server). If a copy of the file has been obtained on the Kaspersky Anti Targeted Attack Platform server, you can click **Find file in Storage** to open the information about the file in Storage.
- **State**—State of the file (whether the file can be restored from Quarantine).

You can click **Restore** to restore the file from Quarantine.

You can click **Get file** to copy the file to the Kaspersky Anti Targeted Attack Platform server.

Clicking the link with the file name or file path opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- **Copy value to clipboard**.

# Restoring an object from Quarantine

*To restore an object from Quarantine on the computer with the Kaspersky Endpoint Agent program:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. In the table, select the object that you want to restore from Quarantine on the computer with the Kaspersky Endpoint Agent program.

   This opens the object details window.
3. Click **Restore** in the lower part of the window.

   This opens the **Tasks** section, the **Restore file from Quarantine** task.
4. In the **Description** field, enter the task description.
5. Click the **Add** button.

The file is restored from Quarantine.

You can also run the task to restore the file from Quarantine by clicking in the right part of the row with object information of the table of objects quarantined on computers with Kaspersky Endpoint Agent.

# Obtaining a copy of a quarantined object on a Kaspersky Anti Targeted Attack Platform server

The file that you want to download a copy of must not exceed 100 MB. If the file exceeds 100 MB, the task does not proceed.

*To copy an object quarantined on a computer with the Kaspersky Endpoint Agent program to a Kaspersky Anti Targeted Attack Platform server:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. In the table, select the object that you want to restore from Quarantine on the computer with the Kaspersky Endpoint Agent program.

   This opens the object details window.
3. Click **Get file** in the lower part of the window.

A copy of the object quarantined on the computer with the Kaspersky Endpoint Agent program is uploaded to the Kaspersky Anti Targeted Attack Platform server. The object is displayed in the **Storage** section, **Files** subsection of the application web interface in the table of objects placed in Storage.

You can also copy an object from Quarantine on a computer with the Kaspersky Endpoint Agent program to the Kaspersky Anti Targeted Attack Platform server by clicking in the right part of the object information row in the table of objects quarantined on computers with Endpoint Agent.

# Removing information about the quarantined object from the table

*To delete the information of an object quarantined on a computer with the Kaspersky Endpoint Agent program from the Kaspersky Anti Targeted Attack Platform table:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. Click the object for which you want to delete information from the table.

   This opens the object details window.
3. Click **Delete**.

   This opens the action confirmation window.
4. Click **Yes**.

The information about the object quarantined on the computer with the Kaspersky Endpoint Agent program is deleted from the table.

You can also delete the information of an object quarantined on a computer with the Kaspersky Endpoint Agent program from the table by clicking in the right part of the object information row in the table of quarantined objects.

# Filtering information about quarantined objects by object description

*To filter the information about quarantined objects by object description:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. Click the **Object** 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 object description.

5. To add a filter condition using a different criterion, click + and specify the filter condition.
6. Click **Apply**.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

## Filtering information about quarantined objects by host name

*To filter the information about quarantined objects by the name of the host where they were quarantined:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. Click the **Update 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 host name.
5. To add a filter condition using a different criterion, click + and specify the filter condition.
6. Click **Apply**.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

## Filtering information about quarantined objects by time

*To filter the information about quarantined objects by the time when they were quarantined:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. 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.
   - **Last hour** if you want the table to display objects that were quarantined during the last hour.

- **Last day** if you want the table to display objects that were quarantined during the last day.
- **Custom range** if you want the table to display objects that were quarantined 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 **Apply**.

The objects table will display only objects matching the filter criteria you have set.

You can use multiple filters at the same time.

# Resetting the filter for information about quarantined objects

*To reset a filter based on one or multiple filter conditions:*

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. Click ✕ to the right of the header of the column of the quarantined objects table for which you want to reset 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.

# 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, create reports based on a template, 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:

1. **Create a report template.**
2. **Create a report based on the template.**

# 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 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.
2. This opens the table of templates. Click the **Add** button.

   This opens the template creation window. 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 **Template 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 **Upload**.

   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 **Apply**.

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 **Apply**.

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 **Apply**.

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.

   This opens the table of reports.

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 **Apply**.

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 **Create**.

The created report is displayed in the table of reports. You can download the report for viewing 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.
   This opens the table of reports.
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.
   This opens the table of reports.
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.
2. This opens the table of templates. Select the template that you want to edit.

   This opens the template editing window.
3. You can edit the following settings:

   - **Template 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 **Apply**.
   - **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.
2. This opens the table of templates. 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 **Apply**.

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.
2. This opens the table of templates. 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 **Apply**.

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.

2. This opens the table of templates. 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 **Apply**.

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.

2. This opens the table of templates. 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.
2. This opens the table of templates. Select the check box in the line containing the template that you want to delete.
3. Click **Delete**.

   This opens the action confirmation window.
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.

   This opens the table of reports.
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 **Apply**.

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.
   This opens the table of reports.
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 **Apply**.

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.
   This opens the table of reports.
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 **Apply**.

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.

   This opens the table of reports.

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.

   This opens the table of reports.

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.
   This opens the table of reports.
2. Select the check box in the line containing the report that you want to delete.
3. Click **Delete**.
   This opens the action confirmation window.
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 **Program 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 **Program 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 **Program 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 **Program 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 **Program 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 **Program 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 **Program settings** tab, **Notifications** section.
2. Click the ⬚ icon in the table of rules for sending notifications.
   This opens the filter configuration window.
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 **Program 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 **Apply**.

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 **Program 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 **Apply**.

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 **Program 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**
   - **Limited functionality**
4. Click **Apply**.

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 **Program 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 **Program 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 **Criteria** drop-down list, select one of the following rule types:

   - **IP**, if you want to add a rule for a computer IP address.
   - **Host**, 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 **Criteria**, 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 **Program 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 **Program settings** tab, **VIP status** section.
2. Select the rule that you want to modify.

   This opens the rule editing window.

3. Make the necessary changes to the **Criteria**, **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 **Program settings** tab, **VIP status** section.
2. Click **Import**.

   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**.

   This opens the file selection window.
4. Select a JSON file containing the list of rules that you want to import and click **Open**.

   This closes the file selection window.

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 **Program 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 **Program settings** tab, **VIP status** section.
2. Click the **Criteria** link to open the filter configuration window.

3. Select one or several check boxes next to the types of rules:
   - **IP**.
   - **Host**.
   - **Email**.
4. Click **Apply**.

   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 **Program 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 **Apply**.

   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 **Program 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 **Apply**.

   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 **Program 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 the white list of objects

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. You can add the following data to the white list:

- **MD5**.
- **Format**
- **URL mask**
- **Email recipient**.
- **Email sender**.
- **Source address or subnet**.
- **Destination address or subnet**.
- **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 **Program settings** section, **White lists** subsection.
2. Go to the **White list** tab.
3. In the upper-right corner of the program web interface window, click the **Add** button.

   This opens the **New record** window.
4. In the **Criteria** drop-down list, select one of the following criteria for adding a record to the white list:

   - **MD5**.
   - **Format**
   - **URL mask**
   - **Email recipient**.
   - **Email sender**.
   - **Source address or subnet**.
   - **Destination address or subnet**.
   - **User agent**.
5. 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.
6. If you selected **MD5**, **URL mask**, **Email recipient**, **Email sender**, **Source address or subnet**, **Destination address or subnet**, or **User agent**, in the **Value** field, enter the value of the relevant criterion that you want to add to the white list:

   - 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 recipient** or **Email sender**, 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 **Source address or subnet** or **Destination address or subnet**, enter the address or subnet in the **Value** field. For example, 255.255.255.0

In the **URL mask**, **Email recipient**, and **Email sender** 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.

7. 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 **Program settings** section, **White lists** subsection.
2. Go to the **White list** tab.
3. 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.
4. In the lower part of the window, click **Delete**.
   The action confirmation window is displayed.
5. 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 **Program settings** section, **White lists** subsection.
2. Go to the **White list** tab.

3. Select the record that you want to modify.

   This opens the **Change notification** window.

4. Make the necessary changes to the **Criteria** and **Value** fields.

5. Click the **Save** button.

The record will be modified.

# Exporting a white list

*To export a white list:*

1. In the main window of the program web interface, select the **Program settings** section, **White lists** subsection.

2. Go to the **White list** tab.

3. 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 by criterion

*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 **Program settings** section, **White lists** subsection.

2. Go to the **White list** tab.

3. Click the **Criteria** link to open the filter configuration window.

4. Select one or more check boxes next to criteria by which you want to filter records:

   - **MD5**.
   - **Format**
   - **URL mask**
   - **Email recipient**.
   - **Email sender**.
   - **Source address or subnet**.

- **Destination address or subnet**.
- **User agent**.

5. Click **Apply**.

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 by value

*To filter or search white list records by value:*

1. In the main window of the program web interface, select the **Program settings** section, **White lists** subsection.
2. Go to the **White list** tab.
3. Click the **Value** link to open the filter configuration window.
4. Enter one or several characters of the value.
5. Click **Apply**.

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 **Program settings** section, **White lists** subsection.
2. Go to the **White list** tab.
3. 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.

# Managing IDS exclusions

You can exclude Kaspersky IDS rules with medium or high importance alerts from scanning. Kaspersky Anti Targeted Attack Platform does not create alerts for excluded IDS rules.

You can add to exclusions only IDS rules defined by Kaspersky. If you do not want to apply a user-defined IDS rule for scanning, you can disable that rule or delete it.

## Viewing the list of IDS rules added to exclusions

*To view the list of IDS rules added to exclusions:*

In the main window of the program web interface, select the **Program settings** section, **White lists** subsection, **IDS exceptions**.

The table of excluded IDS rules is displayed. You can filter the rules by clicking links in column headers.

The table contains the following information:

- **Time created**—Date and time when the IDS rule was added to exclusions.
- **Rule name**—Name of the IDS rule.
- **Rule ID**—ID of the IDS rule. sid (signature ID) in Suricata format.
- **Description**—Description of the IDS rule.
- **Created by**—Name of the user whose account was used to add the IDS rule to exclusions.

## Adding an IDS rule to exclusions

You can exclude Kaspersky IDS rules with medium or high importance alerts from event scanning.

You can add to exclusions only IDS rules defined by Kaspersky. If you do not want to apply a user-defined IDS rule for event scanning, you can disable that rule or delete it.

*To add an IDS rule to exclusions:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

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 the **(IDS) Intrusion Detection System** technology.
5. Click **Apply**.
6. Click to expand the filter settings list.
7. Select one or both alert importance levels:
   - **Medium**—Alert has a medium level of importance.
   - **High**—Alert has a high level of importance.

   The table displays alerts of medium and/or high importance levels generated by the Intrusion Detection System technology based on IDS rules defined by Kaspersky.
8. Select an alert for which the **Detected** column displays the name of the relevant IDS rule.

   This opens a window containing information about the alert.
9. In the right part of the window, in the **Recommendations** section, **Qualifying** subsection, click **Add to exceptions**.

   This opens the **Add IDS rule to exceptions** window.
10. In the **Description** field, enter a description for the IDS rule.
11. Click **Add server**.

The IDS rule is added to exclusions and is displayed in the exclusion list in the **Program settings** section, **White lists** subsection on the **IDS exceptions** in the program web interface. This rule is no longer used for creating alerts.

# Editing the description of an IDS rule added to exclusions

*To edit the description of an excluded IDS rule, in the Alerts section:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.
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 the **(IDS) Intrusion Detection System** technology.
5. Click **Apply**.
6. Click to expand the filter settings list.

7. Select one or both alert importance levels:

   - **Medium**—Alert has a medium level of importance.
   - **High**—Alert has a high level of importance.

   The table displays alerts of medium and/or high importance levels generated by the Intrusion Detection System technology based on IDS rules defined by Kaspersky.

8. Select an alert for which the **Detected** column displays the name of the relevant IDS rule.

   This opens a window containing information about the alert.

9. In the right part of the window, in the **Recommendations** section, **Qualifying** subsection, click **Edit IDS exception**.

   This opens the **Edit IDS exception** window.

   In the **Description** field, edit the description of the rule.

   Click **Save**.

The description of the excluded IDS rule is changed. This rule is no longer used for creating alerts.

# Removing a IDS rule from exclusions

You can remove from exclusions a single IDS rule, multiple rules, or all rules at the same time.

*To remove an IDS rule from exclusions:*

1. In the program web interface window, select the **Program settings** → **White lists** section and go to the **IDS exceptions** tab.
2. A list of excluded IDS rules is displayed.
3. Select the rule that you want to remove from exclusions.

   This opens a window containing information about the rule.

4. Click **Delete**.

   This opens the action confirmation window.

5. Click **Yes**.

The rule is removed from exclusions. The rule is no longer used for creating alerts.

*To remove all or multiple IDS rules from exclusions:*

1. In the program web interface window, select the **Program settings** → **White lists** section and go to the **IDS exceptions** tab.
2. A list of excluded IDS rules is displayed.
3. Select check boxes next to rules that you want to remove from exclusions.

   You can select all rules by selecting the check box in the line containing the headers of columns.

4. In the pane that appears in the lower part of the window, click **Delete**.

   This opens the action confirmation window.

5. Click **Yes**.

The selected rules are removed from exclusions. The rules are no longer used for creating alerts.

# Managing TAA exclusions

You can add TAA (IOA) rules to exclusions. Kaspersky Anti Targeted Attack Platform does not create alerts for such rules and does not display events in which such TAA (IOA) rules are triggered.

## Viewing the list of TAA (IOA) rules added to exclusions

*To view the list of TAA (IOA) rules added to exclusions:*

In the main window of the program web interface, select the **Program settings** section, **White lists** subsection, **TAA exceptions**.

The table of excluded TAA (IOA) rules is displayed. You can filter the rules by clicking links in column headers.

The table contains the following information:

1. —Importance level that is assigned to an alert generated using this TAA (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 which generated it in distributed solution 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** is the name of the rule.

# Viewing a TAA (IOA) rule added to exclusions

*To view the TAA (IOA) rule that was added to exclusions:*

1. In the program web interface window, select the **Program settings** section, **White lists** subsection and go to the **TAA exceptions** tab.
2. The table of excluded TAA (IOA) rules is displayed.
3. Select the rule that you want to view.

   This opens a window containing information about the rule.

The window contains the following information:

- **TAA (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 experts.
- **Confidence** is the level of confidence depending on the probability of false positives as estimated by Kaspersky experts.

# Removing a TAA (IOA) rule from exclusions

You can remove from exclusions a single TAA (IOA) rule, multiple rules, or all rules at the same time.

*To remove a TAA (IOA) rule from exclusions:*

1. In the program web interface window, select the **Program settings** section, **White lists** subsection and go to the **TAA exceptions** tab.
2. The table of excluded TAA (IOA) rules is displayed.
3. Select the rule that you want to remove from exclusions.

   This opens a window containing information about the rule.
4. Click **Delete**.

   This opens the action confirmation window.
5. Click **Yes**.

The rule is removed from exclusions. The rule is applied when creating alerts or scanning events.

*To remove all or multiple TAA (IOA) rules from exclusions:*

1. In the program web interface window, select the **Program settings** section, **White lists** subsection and go to the **TAA exceptions** tab.
2. The table of excluded TAA (IOA) rules is displayed.
3. Select check boxes next to rules that you want to remove from exclusions.

   You can select all rules by selecting the check box in the line containing the headers of columns.
4. In the pane that appears in the lower part of the window, click **Delete**.

   This opens the action confirmation window.
5. Click **Yes**.

The selected rules are removed from exclusions. The rules are applied when creating alerts or scanning events.

# Adding a TAA (IOA) rule to exclusions

You can add to exclusions only TAA (IOA) rules made by Kaspersky. If you do not want to apply a user-defined TAA (IOA) rule for scanning events, you can disable that rule or delete it.

*To add a TAA (IOA) rule to exclusions from the **Alerts** section:*

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.
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 the **(TAA) Targeted Attack Analyzer** technology.
5. Click **Apply**.

   The table displays alerts generated by the TAA technology based on TAA (IOA) rules.
6. Select an alert for which the **Detected** column displays the name of the relevant 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. To the right of the **TAA exceptions** setting name, click **Add to exceptions**.

   This opens a window that allows you to add the TAA (IOA) rule to exclusions.
9. Click **Add server**.

The TAA (IOA) rule is added to exclusions and is displayed in the exclusion list in the **Program settings** section, **White lists** subsection on the **TAA exceptions** tab in the program web interface. This rule is no longer used for creating alerts.

*To add a TAA (IOA) rule to exclusions from the **Threat Hunting** section:*

1. Select the **Threat Hunting** section in the program web interface window.

   This opens the event search form.

2. Define the search conditions and click the **Search** button. For example, you can select event search criteria in the **TAA properties** group in design mode.

   The table of events that satisfy the search criteria is displayed.

3. Select an event.

4. To the right of the **IOA tags** setting, click the name of the rule.

   This opens a window containing information about the rule.

5. To the right of the **TAA exceptions** setting name, click **Add to exceptions**.

   This opens a window that allows you to add the TAA (IOA) rule to exclusions.

6. Click **Add server**.

The TAA (IOA) rule is added to exclusions and is displayed in the exclusion list in the **Program settings** section, **White lists** subsection on the **TAA exceptions** tab in the program web interface. This rule is no longer applied when scanning events.

# 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 **Program 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 **Apply**.

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.

# Managing Kaspersky Endpoint Agent

Kaspersky Endpoint Agent is installed on individual devices in the organization's IT infrastructure that are running under Microsoft Windows operating system. The application constantly monitors the processes running on these devices, open network connections and the files being modified.

Kaspersky Endpoint Agent provides the protected device's interaction with other Kaspersky solutions to detect comprehensive threats (such as targeted attacks).

Kaspersky Endpoint Agent 3.8, which is part of Kaspersky Endpoint Detection and Response Expert solution, supports interaction with Kaspersky Anti Targeted Attack Platform (KATA) and Kaspersky Sandbox.

The application interacts with Kaspersky Anti Targeted Attack Platform using the KATA Central Node component. When integration of Kaspersky Endpoint Agent with KATA Central Node is configured, the application executes the tasks and applies the settings received from the KATA Central Node component, and sends telemetry data from the protected device to the server with the KATA Central Node component.

When integration of Kaspersky Endpoint Agent with Kaspersky Sandbox is configured, the application provides communication between EPP and Kaspersky Sandbox, as well as actions to automatically respond to detected threats (for example, starts critical areas scan on the device or quarantines suspicious objects).

# Installing and uninstalling Kaspersky Endpoint Agent

This section contains information on how to install Kaspersky Endpoint Agent on a device, how to update the application from the previous version, and how to remove the application from a device.

## Preparing for Kaspersky Endpoint Agent installation

Before installing Kaspersky Endpoint Agent on a device or updating the application from the previous version, make sure, that the following conditions are met:

- The device complies with the hardware and software requirements.
- You have the permissions, required for the application installation.

If any of these conditions is not met, the corresponding notification is displayed.

## Installing Kaspersky Endpoint Agent

Kaspersky Endpoint Agent installation can be performed:

- Locally using the Installation Wizard.
- Locally using the command line.

- Remotely using Kaspersky Security Center (for details, refer to Kaspersky Security Center Help).
- Remotely using Microsoft Windows Group Policy Management Editor (for details, visit the Microsoft Technical Support website).

For remote installation, the settings can be passed using the install_props.json configuration file. For this purpose, first place the install_props.json file into the same folder as the endpointagent.msi file.

Installation settings cannot be configured using the install_props.json configuration file if this file was modified manually. To modify the installation settings, create a custom application installation package in Kaspersky Security Center or install the application remotely using Microsoft Windows group policies. If a password must be specified to install the new application version over the previous one, it is recommended to disable password protection during the installation of the application.

# Installing Kaspersky Endpoint Agent using the Installation Wizard

The interface of the application Installation Wizard consists of a sequence of windows corresponding to the application installation steps.

*To install the application or update it from a previous version using the application Installation Wizard,*

copy the endpointagent.msi file which is included in the distribution kit to the user device and run it.

The application Installation Wizard starts.

After Kaspersky Endpoint Agent is installed on the device, the Installation Wizard can be launched on this device in one of the following modes:

- **Modify** the settings of the installed application.
- **Restore** the damaged application modules.
- **Uninstall** the application from the device.

# Updating Kaspersky Endpoint Agent from the previous version

If Kaspersky Endpoint Agent 3.8 is installed on a device with a previous version of Kaspersky Endpoint Agent, all the data that can be migrated is saved and used during Kaspersky Endpoint Agent 3.8 installation, and the previous version of the application is automatically uninstalled.

If Endpoint Sensor version 3.6.X is installed and used on the device as part of Kaspersky Endpoint Security, it is recommended to disable Endpoint Sensor before installing Kaspersky Endpoint Agent in order to avoid possible conflicts between the applications.

When updating a previous version of Kaspersky Endpoint Agent, protected by the password, you must pass this password to the installer by one of the following ways:

- When installing the application locally using the installation wizard interface or interactively using the command line, specify the password at the appropriate step.
- When installing the application locally using the command line in the quiet mode, specify the password as the value of the `UNLOCK_PASSWORD` key.
- When installing the application remotely using Kaspersky Security Center, pass the current password in the installation package settings.

# Repairing Kaspersky Endpoint Agent

If you launch Kaspersky Endpoint Agent installer in the Repair mode, it will check and restore the integrity of all damaged application modules and system registry keys created during application installation.

You can run the installer in the Repair mode in one of the following ways:

- Locally using Kaspersky Endpoint Agent Installation Wizard.
- Locally using the command line.
- Remotely using Kaspersky Security Center by performing one of the following actions (for details, refer to Kaspersky Security Center Help):
  - By selecting the **Repair application if it is already installed** check box when creating the installation package.
  - By specifying the `REINSTALL=ALL` parameter when creating a custom installation package.

If Kaspersky Endpoint Agent installer is launched in the Repair mode and *the application repair is not required*, the installer does not perform any changes on the device.

If Kaspersky Endpoint Agent installer is launched in the Repair mode and *the application is not installed on the device*, application installation will start.

If the Kaspersky Endpoint Agent installer is launched in the Repair mode locally using the command line or remotely using Kaspersky Security Center, and the *settings of the installed application differ from the settings specified in the installer*, the installer will be launched in the mode for changing the settings of the installed application.

# Changes in the system after Kaspersky Endpoint Agent installation

Windows Installer service performs the following changes on the protected device during Kaspersky Endpoint Agent installation:

- Creates Kaspersky Endpoint Agent folders.
- Registers Kaspersky Endpoint Agent keys in the system registry.
- Registers Kaspersky Endpoint Agent services and drivers.

## Kaspersky Endpoint Agent folders on the protected device

When Kaspersky Endpoint Agent is installed, the following folders are created on the device:

- The default Kaspersky Endpoint Agent installation folder that contains Kaspersky Endpoint Agent executable files:
  - In 32-bit version of Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\
  - In 64-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\
- Folder containing Kaspersky Endpoint Agent (x86) drivers:
  - In 32-bit version of Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\drivers\<OS version>\<driver name>
  - In 64-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\drivers\x64\\<OS version>\<driver name>
- Folders containing IOC files:
  - In 32-bit version of Microsoft Windows:
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\openioc\1.1
  - In 64-bit version of Microsoft Windows:
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.0
    - %ProgramFiles%\Kaspersky Lab\Endpoint Agent\openioc\1.1

- Folders containing Kaspersky Endpoint Agent system files:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Images
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kafka
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kata
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Kmp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Cache\Queue\Syslog
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Data\Hunts
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Settings
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\DSKM
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Temp\Tasks
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Bases
- Folder containing system files for Kaspersky Security Network operation.
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Ksn
- Folder containing quarantined files:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Quarantine
- Folder containing files restored from the quarantine:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Restored
- Folder containing Kaspersky Security Center policy configuration files:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Policy
- Folders containing system files for Kaspersky Sandbox operation:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Sandbox\Queue

- Folder containing files of updatable components:
  - %ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0\Update
- Folder containing shortcut files for the Start menu:
  - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Kaspersky Endpoint Agent

## Kaspersky Endpoint Agent services and drivers

The following Kaspersky Endpoint Agent services are registered and started under the system account (SYSTEM):

- SOYUZ.exe is the main Kaspersky Endpoint Agent service that manages its tasks and operation processes.
- VOSTOK.dll (executed in proton.exe) is a service that provides interaction between Kaspersky Endpoint Agent and the Central Node component.
- ANGARA.dll (executed in proton.exe) is a service that provides interaction between Kaspersky Endpoint Agent and EPP in scenarios of Kaspersky Sandbox integration.

The following Kaspersky Endpoint Agent drivers are registered on the device:

- klsnsr.sys is Event Tracing for Windows (ETW) driver.
- klncap.sys is ETW network packet analyzer.

## System registry keys

As a result of Kaspersky Endpoint Agent installation, the following registry keys are created:

- [HKEY_CURRENT_USER SOFTWARE\KasperskyLab\SOYUZ\StartMenu]
- [HKEY_CURRENT_USER SOFTWARE\KasperskyLab\SOYUZ\UninstallShortcut1]
- [HKEY_CURRENT_USER SOFTWARE\KasperskyLab\SOYUZ\UninstallShortcut2]
- [HKEY_CURRENT_USER SOFTWARE\KasperskyLab\SOYUZ\RelNotes]
- [HKEY_CURRENT_USER SOFTWARE\KasperskyLab\SOYUZ\License]
- [HKEY_CURRENT_USER SOFTWARE\KasperskyLab\SOYUZ\ProductUrl]
- [HKEY_LOCAL_MACHINE SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\ConnInstalled]
- HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0\ProdDisplayNa
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0\ProdVersion]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0\ConnectorVe

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0\ConnectorFla
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0\NagentMinVe
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0\ConnectorPa
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0\Installer\UninstallString3]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0\Installer\UninstallString3KI
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0\Installer\ProductCode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\ProgramDataPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLCID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallPlatformType]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\Version]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration(Example)]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SOYUZ]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncap]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klsnsr]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\SOYUZ\4.0\Environment]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vostok]

# Removing Kaspersky Endpoint Agent using the Installation and Uninstallation Wizard

You can uninstall Kaspersky Endpoint Agent using standard Microsoft Windows installation and uninstallation tools. To uninstall the application, a wizard is launched. As a result of its operation all application components are removed from the device.

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

# Installing, restoring and uninstalling the application using the command line

Kaspersky Endpoint Agent can be installed and uninstalled using the msi package, by setting the values of MSI properties in a standard way. For more information on using standard Windows Installer commands and keys, refer to the documentation provided by Microsoft.

## Installing Kaspersky Endpoint Agent

An example of installing the application in the quiet mode with the default settings is shown below. After starting the application installation in the quiet mode, your participation in the installation process is not required.

Installing Kaspersky Endpoint Agent in the quiet mode requires acceptance of the terms and conditions of End User License Agreement and Privacy Policy. Use the `EULA=1` and `PRIVACYPOLICY=1` parameters only if you have fully read, understood and accept the terms of the End User License Agreement and Privacy Policy.

Example:

```
msiexec /i endpointagent.msi EULA=1 PRIVACYPOLICY=1 /qn
```

## Repairing Kaspersky Endpoint Agent

An example of restoring the application in the quiet mode is shown below. After starting the application restoration in the quiet mode, your participation in the restoration process is not required.

Example:

```
msiexec /i endpointagent.msi REINSTALL=ALL /qn
```

### Uninstalling Kaspersky Endpoint Agent

An example of uninstalling the application in the quiet mode is shown below. After starting the application uninstallation in the quiet mode, your participation in the uninstallation process is not required.

Example:
```
msiexec /i {2B71B95B-A56B-4B7C-AFFD-EB731B288EDF} REMOVE=ALL /qn
```
If the application is protected by the password:
```
msiexec /i {2B71B95B-A56B-4B7C-AFFD-EB731B288EDF} REMOVE=ALL UNLOCK_PASSWORD=<password> /qn
```

All data that is stored locally on the device, except for trace and dump files, is deleted from the device when the application is uninstalled.

# Kaspersky Endpoint Agent activation

This section contains information about Kaspersky Endpoint Agent activation.

## Managing Kaspersky Endpoint Agent activation

You can activate Kaspersky Endpoint Agent in one of the following ways:

- During the application installation or update:
  - By specifying the key file at a certain step of the Installation Wizard.
  - By placing the key file in the same folder with the endpointagent.msi file before starting the application installation in the quiet mode (including remote installation).
  - By specifying the path to the key file using the `LICENSEKEYPATH` parameter when installing the application in the quiet mode (including remote installation).

    If there are several key files in the folder, Kaspersky Endpoint Agent will be activated using the key file with the latest license expiration date.

    If Kaspersky Endpoint Agent installer does not detect a key file suitable for Kaspersky Endpoint Agent activation, the application will be installed without activation.
- After the application installation:
  - Using the application activation task in Kaspersky Security Center.
  - Through the command line locally on the device.

You can use Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation.

You can view information about the current license in Kaspersky Security Center in the **Kaspersky licenses** section, in the device properties or through the command line.

For detailed information on managing licenses using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

After the license expires, the application continues to work in limited functionality mode.

# Functional limitations after the license expiration

When the license expires, the following limitations arise in the operation of Kaspersky Endpoint Agent functional components:

- Execution of the jobs received from the Central Node component and the sending the results to the Central Node component is stopped.

  The application sends a message to the Central Node component that the activation status of Kaspersky Endpoint Agent is changed.

  Connection with the Central Node component is not broken. Kaspersky Endpoint Agent continues to accept jobs for creating tasks and changing settings from the Central Node component, but it does not start these tasks and does not enable network isolation and Execution prevention.

- Telemetry is not sent.

- Network isolation cannot be enabled.

  If network isolation was enabled when the license expired, the application disables network isolation in accordance with the specified settings for automatic disabling of network isolation.

- Execution prevention cannot be enabled.

  If Execution prevention was enabled when the license expired, the application stops blocking objects that fall under the specified Execution prevention rules.

- The following tasks stop and cannot be started: Get file, Run process, Terminate process, Delete file.

- The Standard IOC Scan tasks stop and cannot be started.

- KSN/KPSN usage terminates.

When you try to use the listed application functional components after the license expires, the application creates the critical `LicenseViolation` event in the Windows event log and in Kaspersky Security Center Administration Server log. When working through the command line, the application returns code `8` (`AccessDenied`).

# Viewing information about the current license

You can view information about the current license in Kaspersky Security Center in the **Kaspersky licenses** section or in the device properties in the **Keys** section. For detailed information on managing licenses using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

*To view information about the current license on a specific device:*

1. Open Kaspersky Security Center Administration Console.
2. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
3. In the workspace, select the **Devices** tab.
4. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
5. Select **Properties** in the device context menu.

   The device properties window opens.
6. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.
7. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.
8. Select the **Keys** section.

Information about the current license is displayed in the window.

# Managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console

Kaspersky Security Center provides centralized solution to the main tasks of managing and maintaining the organization's network protection system. The application provides the administrator with access to detailed information about the security level of the organization's network and allows configuring all the components of protection built based on Kaspersky applications.

Kaspersky Security Center enables remote installation, uninstallation, start and stop of Kaspersky Endpoint Agent, as well as configuration of the application settings, and start and stop of the application tasks. Kaspersky Security Center provides differentiation of access permissions to Kaspersky Endpoint Agent using the Role Based Access Control (RBAC) technology.

For detailed information on Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

User interface for working with Kaspersky Security Center is provided by means of *Kaspersky Security Center Administration Console* (hereinafter also referred to as *Administration Console*). Administration Console is implemented as an extension component to the Microsoft Management Console (MMC).

Kaspersky Endpoint Agent is managed in Kaspersky Security Center Administration Console using *Kaspersky Endpoint Agent Management plug-in*.

This section contains the basic information about managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console.

# Managing Kaspersky Endpoint Agent policies

This section describes how to create Kaspersky Endpoint Agent policy and enable policy settings.

## Creating Kaspersky Endpoint Agent policy

*To create a Kaspersky Endpoint Agent policy in Kaspersky Security Center:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Click **Create a policy**.

   The policy creation wizard starts.
4. In the **Enter group policy name** window, perform the following actions:
   a. Enter the name that will be used for the new policy in the policy list.
   b. If you want to import the settings of an existing Kaspersky Endpoint Agent policy to a new policy, perform the following actions:
      1. Select the **Use the policy settings for previous application version** check box.
      2. Click **Select** and in the window that opens, select the policy whose settings you want to import.
      3. Click **OK**.
   c. Click **Next**.
5. In the **Create Policy** window, select one of the following options and click **Next**:
   - **Create a new policy and configure settings**.
   - **Create a new policy with default settings**.

   If you select the **Use the policy settings for previous application version** check box at the previous step, the **Create a new policy and configure settings** option is selected by default, and the settings specified in the imported policy are displayed during the policy creation. In this case, the switch in the upper right corner of each section with the policy settings, that shows if the policy is applied, depends on the position of the switches in the groups of settings of the imported policy.
6. In the **Select policy type** window, select the required Kaspersky Endpoint Agent deployment method by selecting the appropriate check boxes and click **Next**.

7. If you select the **Create a new policy and configure settings** option, perform one of the following actions in all sequentially displayed settings windows:

   - To configure the application settings in displayed sections during the policy creation:

     a. Click **Configure** next to the name of the required section.

     b. In the window that opens, configure the required settings and click **OK**.

     c. Click **Next**.

   - To configure the application settings in the displayed section later, click **Next**.

   Configuration of the application settings consists of the following steps:

   > The composition of the steps depends on the type of policy selected at the previous step and may differ from the one described.

   - Configuring integration between Kaspersky Endpoint Agent and Kaspersky Sandbox.
   - Configuring integration between Kaspersky Endpoint Agent and the KATA Central Node component.
   - Configuring threat response settings.
   - Configuring application repositories.
   - Configuring application security settings.
   - Configuring general application settings.

8. In the **Target group** window, select Kaspersky Security Center administration group to which the created policy will be applied by performing the following steps:

   a. Click **Browse**.

   The administration group selection window opens.

   b. Select the administration group from the list.

   For example, you can select the **Managed devices** group.

   c. If you want to create a subgroup in the **Managed devices** group:

      1. Click **New group**.
      2. In the window that opens, enter the name of the device subgroup.
      3. Click **OK**.

   d. Click **Next**.

9. In the **Creating a group policy for the application** window select one of the following policy statuses:

    - **Active policy** to activate the policy immediately after creation.
    - **Inactive policy** to activate the policy later.

10. Select the **Open policy properties after creation** check box, if you want to perform additional configuration of the policy immediately after creation.
11. Click **Done**.

The created policy appears in the policy list.

## Enabling settings in Kaspersky Endpoint Agent policy

When you configure Kaspersky Endpoint Agent policy settings, by default these settings are saved, but are not applied until you enable them.

You can enable settings for the groups where these settings are located. You can enable either individual groups of settings or all groups of settings within one policy.

*To enable the group of settings in Kaspersky Endpoint Agent policy:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.

4. Select the policy for which you want to enable the settings.
5. In the window that opens, select the section and group of settings to which the required setting belongs.
6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

    All the settings of the group will be applied in the policy.

# Configuring Kaspersky Endpoint Agent settings

This section describes how to configure Kaspersky Endpoint Agent settings using the Management plug-in.

*To open Kaspersky Endpoint Agent settings window:*

1. Open Kaspersky Security Center Administration Console.
2. Expand the **Managed devices** node in Kaspersky Security Center Administration Console tree.
3. Select the administration group for which you want to configure application settings.
4. Perform one of the following actions in the details pane of the selected administration group:
   - To configure the application settings for a group of devices, select the **Policies** tab and open the **Properties: <Policy name>** window by double-clicking the policy name or by selecting **Properties** in the context menu.
   - To configure the application settings for a single device, select the **Devices** tab and perform the following actions:
     a. Open the **Properties: <Device name>** window by double-clicking the device name or by selecting **Properties** in the context menu.
     b. Select the **Applications** section.
     c. Open the **Application settings** window by double-clicking the application name or by clicking the **Properties** button under the list of applications.

If an active Kaspersky Security Center policy is applied to a device and blocks changes to the application settings, then these settings cannot be edited in the **Application settings** window.

# Configuring Kaspersky Endpoint Agent security settings

To ensure maximum security of the IT infrastructure in your organization, you can configure access of users and third-party processes to Kaspersky Endpoint Agent. To do so, you can:

- Restrict user permissions to manage the application settings and services.
- Protect actions in the application with a password.
- Enable the application self-defense mechanism.

## Configuring user permissions

You can grant access to Kaspersky Endpoint Agent to individual users or groups of users. As a result, only specified users will be able to manage settings or services of the application.

*To configure user permissions:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Application settings** section select the **Security settings** subsection.
5. In the **User permissions** group of settings, click the **Configure** button next to the name of the required setting.

    The permissions window for Kaspersky Endpoint Agent group opens.
6. In the upper block of settings for groups or users, select the group or user to which you want to grant permissions.
7. In the lower block of permission settings for groups or users, select check boxes in items with the required permissions.
8. Click **OK**.
9. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
10. In the policy properties window, click **OK**.

User permissions for managing the application settings and services are configured.

## Enabling Password protection

Unrestricted user access to the application and its settings can reduce the security level of the device. Password protection allows to limit user access to the application.

*To enable password protection:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Application settings** section select the **Security settings** subsection.
5. In the **Password protection** group of settings select the **Apply password protection** check box.
6. Enter a password and confirm it.

It is recommended to select the password that meets the following requirements:

- Password must be at least 8 characters long.
- Password must not contain user account name.
- Password must not match the name of the device on which Kaspersky Endpoint Agent is installed.
- Password must contain characters from at least three of the following groups:
  - uppercase characters (A-Z);
  - lowercase characters (A-Z) (a-z);
  - numbers (0-9);
  - special characters (!$#%).

7. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
8. Click **OK**.

Password protection is enabled. If a user attempts to perform a password protected action, the application prompts the user to enter the password.

The application does not check the strength of the specified password. We recommend that you use third-party tools to verify the strength of the password. The password is considered strong enough, if verification results confirm that the password cannot be guessed for at least 6 months.

The application does not prohibit from entering password after many attempts of entering incorrect password.

## Enabling and disabling Self-Defense

The Self-Defense mechanism of Kaspersky Endpoint Agent provides protection from malware that tries to lock the application or delete it. The Self-Defense mechanism prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

*To enable or disable Self-Defense:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Application settings** section select the **Security settings** subsection.

5. In the **Self-defense** group of settings, do one of the following:

   - Select the **Enable self-defense for application modules in memory** check box to enable the self-defense mechanism.

   - Clear the **Enable self-defense for application modules in memory** check box to disable the self-defense mechanism.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

7. Click **OK**.

The Self-Defense mechanism is enabled or disabled.

## Configuring Kaspersky Endpoint Agent connection settings to a proxy server

Proxy server connection settings are used for updating databases, activating the application, and external services.

If you use Nginx as a proxy server, configure the `client_max_body_size` setting: the value of the `client_max_body_size` setting must be equal to the maximum size of the object sent by Kaspersky Endpoint Agent to Kaspersky Sandbox for processing. Otherwise, Nginx will not send the objects whose size exceeds the specified value. The default value is 1 MB.

*To configure proxy server connection settings:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.

   - Select **Properties** in the policy context menu.

   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Application settings** section select the **Other settings** subsection.

5. Select one of the following proxy service usage options:

   - **Do not use proxy server**.

   - **Use proxy server with specified settings**.

6. If you select the **Use proxy server with specified settings** option, specify the address and port of the proxy server you want to connect to in the **Server name or IP address** and **Port** fields.

   The default port number is 8080.

7. If you want to use NTLM authentication for connecting to the proxy server:

    a. Select the **Use NTLM authentication by user name and password** check box.

    b. In the **User name** field, enter the name of the user, whose account will be used for proxy server authentication.

    c. In the **Password** field, enter the password for connecting to the proxy server.

    You can make password characters visible by clicking **Show** to the right of the **Password** field.

8. If you do not want to use the proxy server for internal addresses of your organization, select the **Bypass proxy server for local addresses** check box.

9. Click the **Apply** button.

    As a result, you return to the policy properties window.

10. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

11. Click **OK**.

Proxy server connection settings are configured.

## Configuring Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation

*To enable usage of Kaspersky Security Center as a proxy server for the application activation:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.

4. In the **Application settings** section select the **Other settings** subsection.

5. In the **Licensing** group of settings, select the **Use Kaspersky Security Center as a proxy server when activating the application** check box.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

7. Click **OK**.

Kaspersky Security Center usage as a proxy server for Kaspersky Endpoint Agent activation is now enabled.

# Configuring KSN and KMP usage in Kaspersky Endpoint Agent

To protect your computer more effectively, Kaspersky Endpoint Security uses data received from users around the globe. Kaspersky Security Network is designed to receive such data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online Kaspersky Knowledge Base that contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Web Traffic Security to objects that are not yet listed in anti-virus application databases, improves performance of some protection components, and reduces the likelihood of false positives.

Participation in Kaspersky Security Network allows Kaspersky to quickly acquire information about the types and sources of objects that are not yet listed in anti-virus application databases, develop methods for neutralizing such objects, and reduce the number of false positives.

When you use Kaspersky Security Network, certain statistical data collected while Kaspersky Endpoint Agent is running is automatically sent to Kaspersky. Files or their parts which may be exploited by intruders to harm the computer or data can be also sent to Kaspersky to be examined additionally.

Kaspersky Managed Protection (also referred to as KMP) is an operational service intended to actively search for cyber threats that are aimed at your organization. As part of the service, Kaspersky CyberSecurity Monitoring Center experts analyze extended telemetry data received from Kaspersky Security for Business and Kaspersky Anti Targeted Attack products installed in the customer's networks and acting as sensors. This information is aggregated using Kaspersky Security Network and is examined by the analysts on the basis of Threat intelligence data collected by Kaspersky during the whole activity period, which makes it possible to detect current tactics, techniques and procedures of cybercriminals.

> No personal data is collected, processed, or stored. The types of data that Kaspersky Endpoint Agent sends to Kaspersky Security Network and Kaspersky Managed Protection are described in KSN Statement and KMP Statement.

Participation in Kaspersky Security Network and Kaspersky Managed Protection is voluntary. KSN and KMP usage is disabled by default. After enabling KSN and KMP usage, you can disable this option at any time.

*To enable KSN and KMP usage:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. Select the **Participation in KSN/KMP** section.
5. Review the KSN Statement.

6. If you agree with terms and conditions of the Statement, select the **I confirm that I have fully read, understand, and accept the terms and conditions of this KSN Statement** check box.

7. Select the **Enable Kaspersky Security Network ("KSN") usage** check box.

8. To enable KMP usage:

    a. Review the KMP Statement.

    b. If you agree with terms and conditions of the Statement, select the **I confirm that I have fully read, understand, and accept the terms and conditions of this KMP Statement** check box.

    c. Select the **Enable Kaspersky Managed Protection ("KMP") usage** check box.

9. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

10. Click **OK**.

KSN and KMP usage is enabled.

# Configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox

This section contains information on configuring the integration of Kaspersky Endpoint Agent with Kaspersky Sandbox. Integration must be configured both on Kaspersky Endpoint Agent side using Kaspersky Security Center Administration Console, and on Kaspersky Sandbox side using the web interface.

## Enabling and disabling integration with Kaspersky Sandbox

*To enable or disable integration with Kaspersky Sandbox:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

    - Double-click the policy name.

    - Select **Properties** in the policy context menu.

    - Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection.

5. In the **Kaspersky Sandbox integration settings** group of settings, do one of the following:

    - Select the **Enable Kaspersky Sandbox integration** check box to enable integration with Kaspersky Sandbox.

    - Clear the **Enable Kaspersky Sandbox integration** check box to disable integration with Kaspersky Sandbox.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

7. Click **OK**.

Integration with Kaspersky Sandbox is enabled or disabled.

## Configuring trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent

You can configure trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent in the web interface of Kaspersky Sandbox server that is *not included in the cluster*.

If you have already merged servers into a cluster, remove the server from the cluster, then create a new cluster based on this server and add all the servers intended for Kaspersky Sandbox solution to the new cluster.

If the servers you need belong of another cluster, remove them from that cluster one by one and then add them to your cluster.

Installing and configuring a trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent involves:

1. **Removing a server from the cluster (if the server belongs to a cluster)**
2. **Generating or uploading to the server a TLS certificate for connection with Kaspersky Endpoint Agent**
3. **Creating a new cluster based on this server**
4. **Removing all the servers that you want to add to this cluster from the clusters they currently belong to**
5. **Adding all required servers to the new cluster**
6. **Adding all servers belonging to Kaspersky Sandbox new cluster to Kaspersky Endpoint Agent list**
7. **Configuring a trusted connection with Kaspersky Sandbox on Kaspersky Endpoint Agent side**

## Configuring the trusted connection on the Kaspersky Sandbox side

To configure a trusted connection, you must generate or upload a TLS certificate in Kaspersky Sandbox, save it on a computer, and then upload it to the Kaspersky Endpoint Agent application.

*To generate a TLS certificate for the connection of Kaspersky Sandbox with Kaspersky Endpoint Agent:*

1. In the window of the Kaspersky Sandbox web interface, select the **TLS certificates** section.

2. In the **TLS certificate for the connection with Kaspersky Endpoint Agent** section, click **Generate**.

   The action confirmation window opens.

3. Click **Yes**

Kaspersky Sandbox generates a new TLS certificate. The page is automatically refreshed.

You can choose to prepare the TLS certificate on your own and upload it using the Kaspersky Sandbox web interface.

The TLS certificate file prepared for upload 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 private key length must be 2048 bits or longer.

For more details on preparing TLS certificates for import, please refer to the documentation on Open SSL.

*To upload the TLS certificate using the Kaspersky Sandbox web interface:*

1. In the window of the Kaspersky Sandbox web interface, select the **TLS certificates** section.
2. In the **TLS certificate for the connection with Kaspersky Endpoint Agent** section, click **Upload**.
   The file selection window opens.
3. Select a TLS certificate file to download and click the **Open** button.
   The file selection window closes.

The TLS certificate is added to Kaspersky Sandbox.

*To save the file of the TLS certificate for the connection with Kaspersky Endpoint Agent on your computer:*

1. In the window of the Kaspersky Sandbox web interface, select the **TLS certificates** section.
2. In the **TLS certificate for the connection with Kaspersky Endpoint Agent** section, click **Download**.

The TLS certificate file is saved in the downloads folder of the browser.

## Configuring trusted connection on Kaspersky Endpoint Agent side

*To configure trusted connection on Kaspersky Endpoint Agent side:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection.
5. In the **Kaspersky Sandbox integration settings** group of settings, select the **Use pinned certificate to secure connection** check box.

6. Click the **Add new TLS certificate** button.

   The **Adding new TLS certificate** window opens.

7. Perform one of the following actions to add a TLS certificate created on Kaspersky Sandbox side:

   - Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one TLS certificate of Kaspersky Sandbox server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.

8. Click **Add**.

   Information about the added TLS certificate is displayed in the **Kaspersky Sandbox integration settings** group of settings.

9. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

10. Click **OK**.

Trusted connection to Kaspersky Sandbox server is configured.

## Updating Kaspersky Sandbox TLS certificate data in Kaspersky Endpoint Agent

When replacing the TLS certificate of Kaspersky Sandbox server, you will need to update TLS certificate data in Kaspersky Endpoint Agent and reconfigure trusted connection with Kaspersky Sandbox.

*To update Kaspersky Sandbox TLS certificate data in Kaspersky Endpoint Agent:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection and the **Kaspersky Sandbox integration settings** group of settings.
5. Select the **Use pinned certificate to secure connection** check box.
6. Click the **Add new TLS certificate** button.

   The **Adding new TLS certificate** window opens.

7. Perform one of the following actions to add a TLS certificate created on Kaspersky Sandbox side:

   - Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one TLS certificate of Kaspersky Sandbox server. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.

8. Click **Add**.

   Information about the added TLS certificate is displayed in the **Kaspersky Sandbox integration settings** group of settings.

9. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

10. Click **OK**.

    As a result, Kaspersky Sandbox server TLS certificate data is updated and trusted connection with Kaspersky Sandbox is established.

## Configuring the response timeout of Kaspersky Sandbox and request queue settings

*To configure the response timeout of Kaspersky Sandbox and processing queue settings for objects that Kaspersky Endpoint Agent sends to Kaspersky Sandbox:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox advanced settings** subsection.
5. In the **Timeout** group of settings, specify the maximum Kaspersky Sandbox response timeout.
6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
7. In the **Kaspersky Sandbox requests queue** group of settings, in the **Queue folder** field specify the path to the folder where information about the requests sent to Kaspersky Sandbox will be stored.
8. In the **Maximum queue size (MB)** field, specify the maximum allowed size of the request queue in megabytes.
9. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
10. Click **OK**.

## Adding Kaspersky Sandbox servers to Kaspersky Endpoint Agent list

If you enabled the integration with Kaspersky Sandbox, you can add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list. You can add several Kaspersky Sandbox servers.

For a particular policy, add servers that are part of the same cluster. If servers belong to different clusters, the outcome is unpredictable.

All servers in the cluster are peers regardless of which server was used as the base for creating the cluster. Processing the same object on any server in the cluster will yield the same result.

Kaspersky Anti Targeted Attack Platform balances load among the servers. Objects that Kaspersky Endpoint Agent sends for processing to Kaspersky Anti Targeted Attack Platform are processed on the least busy server.

To make Kaspersky Anti Targeted Attack Platform cluster process objects from Kaspersky Endpoint Agent, add to Kaspersky Endpoint Agent at least one server that is part of the cluster during the integration of Kaspersky Endpoint Agent with Kaspersky Anti Targeted Attack Platform.

The list of Kaspersky Anti Targeted Attack Platform servers of Kaspersky Endpoint Agent displays only the servers that you added to this list. Nevertheless, objects can be processed by any server in the cluster thanks to load balancing. The current list of servers in the cluster is displayed in the web interface of Kaspersky Anti Targeted Attack Platform.

It is recommended to add all servers of the cluster to Kaspersky Endpoint Agent.

Kaspersky Endpoint Agent can connect to a different Kaspersky Anti Targeted Attack Platform server in the list if one of the following errors occurs:

- Kaspersky Anti Targeted Attack Platform response timeout (connection timeout).
- Kaspersky Anti Targeted Attack Platform is not available (error code 503 or 504).
- Self-diagnosis problem other than a license problem (error code 500).

When removing a server from the cluster, the following object processing scenarios are possible:

- If there is at least one server from this cluster with a valid IP address or fully qualified domain name (FQDN) in the list of Kaspersky Anti Targeted Attack Platform servers of Kaspersky Endpoint Agent, Kaspersky Anti Targeted Attack Platform continues processing objects from Kaspersky Endpoint Agent.
- If no servers from this cluster remain in the list of Kaspersky Anti Targeted Attack Platform servers of Kaspersky Endpoint Agent, or if IP addresses or fully qualified domain names of cluster servers are not valid, Kaspersky Anti Targeted Attack Platform cannot receive and process objects from Kaspersky Endpoint Agent.

  For correct processing of objects, at least one server from Kaspersky Anti Targeted Attack Platform cluster must be added to Kaspersky Endpoint Agent.

*To add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Kaspersky Sandbox integration settings** subsection.
5. Select the **Enable Kaspersky Sandbox integration** check box if it is cleared.
6. In the **List of Kaspersky Sandbox servers** group of settings, click **Add**.

   The **Server properties** window opens.
7. Enter the IP address or fully qualified domain name of Kaspersky Sandbox server and the port used for connecting to the server.
8. Click **Add**.

   The added server is listed in the server table.
9. Repeat the steps to add each Kaspersky Sandbox server to the list.
10. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
11. Click **OK**.

Kaspersky Sandbox servers are added to Kaspersky Endpoint Agent list.

## Configuring Threat Response actions of Kaspersky Endpoint Agent to respond to threats detected by Kaspersky Sandbox

Kaspersky Endpoint Agent can perform actions in response to threats detected by Kaspersky Sandbox.

You can configure the following types of actions:

- *Local* – actions to be performed on each device where a threat is detected.
- *Group* – actions to be performed on all devices of the administration group for which the policy is configured.

Local actions:

- **Quarantine and delete**.

  When a threat is detected on a device, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

- **Notify device user**.

  When a threat is detected on a device, a notification about the detected threat is displayed to the device user.

  The notification is displayed if the device is running under the user account same to the account under which the threat was detected.

  If the device is not running or is running under another user account, the notification is not displayed.

- **Push Endpoint Protection Platform (EPP) scanning on critical areas**.

  If a threat is detected on a device, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas of the device. Critical areas include kernel memory, objects loaded at operating system startup, and boot sectors of the hard drive. For more details on configuring the scan settings refer to the documentation of EPP being used.

Group actions:

- **Run IOC scanning on a managed group of hosts**.

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat.

- **Quarantine and delete when IOC is detected**.

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent scans all devices of this administration group for objects containing the detected threat. When an object which contains a threat is detected on devices of this administration group, a copy of the object containing the threat is quarantined, and the object is deleted from the device.

- **Push Endpoint Protection Platform (EPP) scanning on critical areas when IOC is detected**.

  If a threat is detected on any device of the administration group for which you configure the policy, Kaspersky Endpoint Agent sends a command to EPP to scan critical areas on all administration group's devices where the object containing the threat was detected. For more details on configuring the scan settings refer to the documentation of EPP being used.

To configure group threat response actions, set up the permissions of Kaspersky Security Center users, whose accounts you want use for managing IOC Scan tasks.

When configuring threat response actions, keep in mind that as a result of some actions, the object containing the threat may be deleted from the workstation where it was detected.

## Enabling and disabling Threat Response actions

*To enable or disable Threat Response actions of Kaspersky Endpoint Agent for reacting to threats detected by Kaspersky Sandbox:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat Response** subsection.
5. In the **Actions** group of settings:
   - Select the **Take response actions on threats, detected by Kaspersky Sandbox** check box to enable Threat Response actions.
   - Clear the **Take response actions on threats, detected by Kaspersky Sandbox** check box to disable Threat Response actions.
6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
7. Click **Apply** and **OK**.

## Adding Threat Response actions to the action list of the current policy

*To add Threat Response actions to the list of actions of the current policy:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat Response** subsection.

5. In the **Actions** group of settings, select the **Take response actions on threats, detected by Kaspersky Sandbox** check box, if it is not selected.

6. Click **Add** and in the drop-down list, select one of the following actions:

   - **Quarantine and delete**. Local action. Performed on the device, where a threat is detected.
   - **Notify device user**. Local action. Performed on the device, where a threat is detected.
   - **Push Endpoint Protection Platform (EPP) scanning on critical areas**. Local action. Performed on the device, where a threat is detected.
   - **Run IOC scanning on a managed group of hosts**. Group action. Performed on all the device of the administration group.
   - **Quarantine and delete when IOC is detected**. Group action. Performed on all the device of the administration group.
   - **Push Endpoint Protection Platform (EPP) scanning on critical areas when IOC is detected**. Group action. Performed on all the device of the administration group.

   The action is added to the **Current actions** list.

   When configuring threat response actions, keep in mind that as a result of some actions, the object containing the threat may be deleted from the workstation where it was detected.

7. To remove an action, select it in the table and click **Remove**.

8. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

9. Click **Apply** and **OK**.

## Authentication for Threat Response group tasks on the Administration Server

If you want Kaspersky Endpoint Agent to create group tasks for Threat Response, perform authentication on the Administration Server: enter the user name and password for connecting to Kaspersky Security Center.

You can authenticate with the internal Kaspersky Security Center user account created in Kaspersky Security Center or use Windows authentication.

For more information about creating Kaspersky Security Center user accounts and Windows authentication, refer to *Kaspersky Security Center Help*.

The user account name must not be the same as the domain name of the user and must not have the `<domain name>\<user name>` format.

*To authenticate at the Administration Server:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat Response** subsection.
5. In the **Authentication on Administration Server** group of settings, in the **Administration Server login** field, enter the name of Kaspersky Security Center user account.
6. In the **Authentication on Administration Server** group of settings, in the **Administration Server password** field, enter the password for accessing Kaspersky Security Center.
7. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
8. Click **OK**.

## Device protection from legitimate applications that can be used by cybercriminals

You can enable detection of legitimate applications that can be used by cybercriminals to harm your organization's local network. Kaspersky Endpoint Agent considers such applications as posing threats and performs threat response actions on them.

*Legitimate applications* are allowed to be installed and used on devices and are designed to perform user tasks. However, some types of legitimate applications, when used by cybercriminals, may harm devices or organization's local network. If cybercriminals gain access to such applications or deploy them on devices, they can use functions of such applications to violate security of the devices or organization's local network.

Such applications include IRC clients, dialers, file download applications, computer system activity monitors, password utilities, Internet servers for FTP, HTTP or Telnet services.

*To enable detection of potentially harmful legitimate applications:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **Kaspersky Sandbox integration** section select the **Threat Response** subsection.
5. In the **Additional** group of settings select the **Enable detection of legitimate applications, which can be exploited by adversaries** check box.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

7. Click **Apply** and **OK**.

Detection of legitimate applications that can be used by cybercriminals to harm your organization's local network is enabled.

## Configuring start of Autonomous IOC Scan tasks

When Kaspersky Sandbox detects a threat, Kaspersky Endpoint Agent automatically creates IOC Scan tasks for all devices (search for MD5 hashes of objects in which the threat was detected).

*To configure start of Autonomous IOC Scan tasks:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Kaspersky Sandbox integration** section select the **Threat Response** subsection.

5. In the **Additional** group of settings click **Configure**.

   The **IOC scanning settings** window opens.

6. In the **Scanning area** group of settings, select one of the following areas where Kaspersky Endpoint Agent will search for IOCs:

   - **File areas, containing system drives**.
   - **Critical file areas**.

7. In the **Scan start** group of settings, select one of the following options to start IOC Scan tasks:

   - **Manual start**. IOC Scan tasks will be created automatically, but will not be started. You can start a single task or all tasks manually.
   - **Immediately on a Kaspersky Sandbox detect**. IOC Scan tasks will be automatically created and started.
   - **Start within the specified period**. IOC Scan tasks will be created automatically, and will be started within the specified period. For example, outside of working hours from 8:00 p.m. to 7:00 a.m.

     If you select the **Start within the specified period** option, specify the start and end of the period in the **Period start time (hh:mm)** *и* **Period end time (hh:mm)** fields.

     All IOC Scan tasks that were automatically created *before the beginning* of the specified period will start at any time *within* the specified period.

All IOC Scan tasks that were automatically created *within* the specified period will start immediately *after creation*.

All IOC Scan tasks that were automatically created *after the end* of the specified period will start *during the next task execution period*.

Example:
If you configured the tasks to run during the period from 8:00 p.m. to 7:00 a.m.:
Tasks that were automatically created at 7 p.m. are started at any arbitrary time from 8:00 p.m. to 7:00 a.m.
Tasks that were automatically created at 9 p.m. are started at 9 p.m.
Tasks that were automatically created at 8:00 a.m. are started during the next task execution period, from 8:00 p.m. to 7:00 a.m.

8. Click **OK**.

   The **IOC scanning settings** window closes.

9. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

10. Click **Apply** and **OK**.

Start of Autonomous IOC Scan tasks is configured.

# Configuring integration between Kaspersky Endpoint Agent and KATA Central Node

This section contains information on how to configure integration between Kaspersky Endpoint Agent and the KATA Central Node component using Kaspersky Security Center Administration Console.

## Configuring data submission settings

*To configure data submission settings:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **General settings** subsection.

5. In the **Data transmission settings** group, do the following:

   - Specify the value in the **Event transmission period (sec.)** field.
   - Specify the value in the **Event limit per one package** field.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
7. Click **OK**.

## Configuring request throttling settings

The request throttling feature allows restricting the flow of events with low importance from Kaspersky Endpoint Agent to the Central Node component.

*To configure the request throttling settings:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **KATA integration** section select the **General settings** subsection.
5. In the **Throttling settings** group of settings, you can perform the following actions:

   - Select or clear the **Enable throttling** check box to enable or disable the feature.

     This feature is enabled by default.

   - Specify the value in the **Maximum events per hour** field.

     The application analyzes telemetry data flow and restricts transmission of events with low importance if the number of transmitted events tends to exceed the value specified in this field. The default value is 3000 events per hour.

   - Specify the value in the **Percent of exceeding the limit of events** field.

     If the flow of events of the same type with low importance exceeds the threshold value specified in this field as a percentage of the total number of events, transmission of events of this type is restricted. The default value is 15%.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

   The default switch position is **Under policy**.

7. Click **OK**.

## Enabling and disabling integration with KATA Central Node

*To enable or disable integration with the KATA Central Node component:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KATA integration settings** subsection.
5. In the **Connection settings** group of settings, do one of the following:
   - To enable integration with KATA Central Node:
     a. Select the **Enable KATA integration** check box.
     b. Specify the IP address or fully qualified domain name of the KATA server and the port used for connecting to the server.
   - To disable integration with KATA Central Node, clear the **Enable KATA integration** check box.
6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
7. Click **OK**.

Integration with KATA Central Node is enabled or disabled.

## Configuring trusted connection with KATA Central Node

*To configure trusted connection between Kaspersky Endpoint Agent and KATA Central Node, perform the following on Kaspersky Endpoint Agent side:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **KATA integration** section select the **KATA integration settings** subsection.

5. In the **Connection settings** group of settings, select the **Use pinned certificate to secure connection** check box.

6. Click the **Add new TLS certificate** button.

   The **Adding new TLS certificate** window opens.

7. Perform one of the following actions to add a TLS certificate:

   - Add a certificate file. Click **Browse**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **Paste TLS certificate data** field.

   Kaspersky Endpoint Agent may have only one KATA server TLS certificate. If you have added a TLS certificate before and then add a TLS certificate once again, only the last added certificate is valid.

8. Click **Add**.

   Information about the added TLS certificate is shown in the **TLS certificate data** group of settings.

9. If you want to configure additional connection protection by a user certificate, click the **Add client certificate** button.

10. In the **Add client certificate** window that opens, do the following:

    a. Select the **Secure connection with client certificate** check box.

    b. Click the **Upload** button and in the window that opens select the PFX archive and click **Open**.

    c. Enter the password for the PFX archive.

    d. Click **OK**.

11. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

12. Click **OK**.

Trusted connection to KATA server is configured.

## Configuring synchronization settings between Kaspersky Endpoint Agent and KATA Central Node

*To configure synchronization settings between Kaspersky Endpoint Agent and KATA Central Node:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
    - Double-click the policy name.
    - Select **Properties** in the policy context menu.
    - Select the **Configure policy settings** item in the right part of the window.
4. In the **KATA integration** section select the **KATA integration settings** subsection.
5. In the **Connection settings** group of settings, configure the following settings:
    - **Timeout (sec.)**. Specify the maximum KATA server response timeout.
    - **Send sync request to KATA server every (min.)**. Specify the time interval for sending requests for synchronization Kaspersky Endpoint Agent settings and tasks with KATA Central Node. You can specify a value from 1 to 60 minutes.
6. Select or clear the **Consider TTL period for events transmission** check box.
7. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.
8. Click **OK**.

# Configure network isolation settings

This section describes how to configure the network isolation settings by means of Kaspersky Endpoint Agent Management plug-in.

## About network isolation in Kaspersky Endpoint Agent

Kaspersky Endpoint Agent provides the ability to isolate devices from the network on demand (manually) or automatically as in response to detections.

After enabling network isolation, the application breaks all active network connections on the devices and blocks all new TCP/IP network connections, except for the connections listed below:

- connections specified as network isolation exclusions;
- connections initiated by the services of compatible EPP;
- connections initiated by the services of Kaspersky Endpoint Agent;
- connections initiated by Kaspersky Security Center Network Agent.

## Enabling and disabling network isolation

Network isolation of the device can be enabled manually or automatically, as a result of response to detections.

Network isolation can be disabled automatically after a specified period of time or manually.

If the **Automatically end device isolation after** check box is not selected in the network isolation settings and the time interval is not specified, network isolation will be disabled automatically after five hours since it was enabled.

After disabling network isolation, the device can work in the network without restrictions imposed by Kaspersky Endpoint Agent during network isolation.

## Network isolation exclusions

You can configure network isolation exclusions. Network connections that meet the conditions of the specified rules will not be blocked on the devices after network isolation is enabled.

To simplify configuration of network isolation exclusions, a list of network profiles (sets of predefined rules) is available in the application. The list and contents of the network profiles cannot be edited.

Exclusions can be specified both as part of network profiles and separately. Exclusions specified separately from the network profiles are called *custom exclusions*.

By default, exclusions include network profiles, consisting of rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles.

If you change the settings of the exclusion that was specified in the network profile, this exclusion will become custom.

Exclusions specified in the policy properties are applied only if network isolation is automatically enabled by the application in response to detection. Exclusions specified in the device properties are applied only if network isolation is enabled manually.

The active policy does not block the usage of network isolation exclusions specified in the device properties, since the scenarios for applying these settings are different.

# About managing network isolation in Kaspersky Endpoint Agent

You can manage network isolation using Kaspersky Security Center Administration Server, using the Central Node component interface, or through the command line interface on the protected device. Information on managing network isolation by all these methods is shown in the next table.

| Management interface | Capabilities | Notes |
|---|---|---|
| Kaspersky Security Center Administration Console | • Enabling and disabling network isolation.<br>• Configuring automatic disabling of network isolation.<br>• Configuring device user notification about network isolation.<br>• Configuring exclusions from network isolation. | The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device.<br>Manual enabling and disabling network isolation for a group of device in a policy is not available. |
| Command line | • Getting information about the current status and settings of the device network isolation. | Network isolation cannot be enabled or disabled and its setting cannot be configured through the command line interface. |
| Central Node component | Network isolation management using the Central Node component is described separately. | Kaspersky Endpoint Agent retains network isolation settings received from the Central Node component in the device properties in Kaspersky Security Center. |

## Enabling and disabling network isolation

*To enable or disable network isolation of a device:*

1. **Open the application properties window for an individual device**.
    1. Open Kaspersky Security Center Administration Console.
    2. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
    3. In the workspace, select the **Devices** tab.
    4. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
    5. Select **Properties** in the device context menu.

       The device properties window opens.
    6. Select the **Applications** section.

       A list of Kaspersky applications installed on the device is displayed in the window.
    7. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
        - Double-click the application name.
        - In the application context menu, select **Properties**.
        - Click the **Properties** button under the list of Kaspersky applications.
2. In the **Network isolation** section select **General settings**.
3. In the **Isolate device** group of settings, select or clear the **Isolate current device from the network** check box.
4. Click **OK** to save the changes.

Manual enabling and disabling network isolation for a group of device in a policy is not available.

## Enabling and disabling user notification about network isolation

The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device.

*To enable or disable the user notification about network isolation:*

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. Open Kaspersky Security Center Administration Console.
     2. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
     3. In the workspace, select the **Devices** tab.
     4. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
     5. Select **Properties** in the device context menu.

        The device properties window opens.
     6. Select the **Applications** section.

        A list of Kaspersky applications installed on the device is displayed in the window.
     7. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:

        - Double-click the application name.
        - In the application context menu, select **Properties**.
        - Click the **Properties** button under the list of Kaspersky applications.

   - **Open the policy properties window**.

     1. Open Kaspersky Security Center Administration Console.
     2. In the console tree, open the **Policies** folder.
     3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

        - Double-click the policy name.
        - Select **Properties** in the policy context menu.
        - Select the **Configure policy settings** item in the right part of the window.

2. In the **Network isolation** section select **General settings**.

3. In the **Notification** group of settings select or clear the **Notify a device user when device is isolated from the network** check box.

4. Click **OK** to save the changes.

## Configuring automatic disabling of network isolation

The settings of automatic network isolation are configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) are configured in the properties of an individual device.

*To configure the settings for automatic disabling of network isolation:*

1. Do one of the following:

- **Open the application properties window for an individual device**.

    1. Open Kaspersky Security Center Administration Console.

    2. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.

    3. In the workspace, select the **Devices** tab.

    4. Select the device for which you want to configure Kaspersky Endpoint Agent settings.

    5. Select **Properties** in the device context menu.

       The device properties window opens.

    6. Select the **Applications** section.

       A list of Kaspersky applications installed on the device is displayed in the window.

    7. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:

        - Double-click the application name.

        - In the application context menu, select **Properties**.

        - Click the **Properties** button under the list of Kaspersky applications.

- **Open the policy properties window**.

    1. Open Kaspersky Security Center Administration Console.

    2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

2. In the **Network isolation** section select **General settings**.
3. In the **Device isolation terms** group of settings, do one of the following:

   - Clear the **Automatically end device isolation after** check box to disable automatic disabling of network isolation after a specified period of time.

     This feature is enabled by default.

   - Select the **Automatically end device isolation after** check box to enable automatic disabling of network isolation after a specified period of time.

4. Specify the period after which network isolation will be disabled.

   The default period is 30 minutes.

5. Click **OK** to save the changes.

If the **Automatically end device isolation after** check box is not selected in the network isolation settings and the time interval is not specified, network isolation will be disabled automatically after five hours since it was enabled.

## Configuring exclusions from network isolation

Exclusions specified in the policy properties are applied only if network isolation is automatically enabled by the application in response to detection. Exclusions specified in the device properties are applied only if network isolation is enabled manually.

The active policy does not block the usage of network isolation exclusions specified in the device properties, since the scenarios for applying these settings are different.

*To configure the settings of network isolation exclusions:*

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. Open Kaspersky Security Center Administration Console.
     2. In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required device.
     3. In the workspace, select the **Devices** tab.

4. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
5. Select **Properties** in the device context menu.
   The device properties window opens.
6. Select the **Applications** section.
   A list of Kaspersky applications installed on the device is displayed in the window.
7. Select Kaspersky Endpoint Agent and open its properties window in one of the following ways:
   - Double-click the application name.
   - In the application context menu, select **Properties**.
   - Click the **Properties** button under the list of Kaspersky applications.

- **Open the policy properties window**.
  1. Open Kaspersky Security Center Administration Console.
  2. In the console tree, open the **Policies** folder.
  3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
     - Double-click the policy name.
     - Select **Properties** in the policy context menu.
     - Select the **Configure policy settings** item in the right part of the window.

2. If you open the application properties window for an individual device, in the **Network isolation** section, select **Exclusion rules**.
3. If you open the application policy properties window, in the **Network isolation** section, select **Isolation on detect**.
4. You can perform the following actions:

   - **Add custom exclusion**

     *To add a custom exclusion:*

     1. Click **Add**.
     2. In the drop-down list select **Add a custom rule**.
        The **Rule properties** window opens.
     3. Specify the required exclusion settings and click **OK**.
        The new rule is added to the exclusion list.

- **Add exclusions from the list of predefined network profiles**

  *To add exclusions from the list of predefined network profiles:*

  1. Click **Add**.
  2. In the drop-down list select **Add from the network profile dictionary**.
  3. In the window that opens, select the required network profile from **Predefined network profiles list**.

     At the bottom of the window, the description of the selected network profile is displayed.
  4. If you want to view the exclusions that will be applied with the selected network profile, click the **Show rules list** button.
  5. If you want to add the selected network profile to the list of applicable profiles, click **-->**.

     You can add several network profiles at once.
  6. Click the **Add selected** button.

     Exclusions from the selected network profiles are added to the list of exclusions.

- **Change the settings of the added exclusion**

  *To change the settings of the added exclusion:*

  1. Select the required exclusion in the **Exclusion rules** list.
  2. Click the **View and edit** button.
  3. The **Rule properties** window opens.
  4. Make the required changes and click **OK**.

  The selected exclusion is changed.

  > If you change the settings of the exclusion that was specified in the network profile, this exclusion will become custom.

- **Enable or disable exclusion**

  *To enable an exclusion,*

  select the check box next to the exclusion name in the **Exclusion rules** list.

  *To disable an exclusion,*

  clear the check box next to the exclusion name in the **Exclusion rules** list.

- **Remove exclusion from the list**

  *To remove an exclusion from the list:*

  1. In the **Exclusion rules** list, select the exclusion you want to remove.
  2. Click the **Remove** button.

  The exclusion is removed from the list of exclusions.

5. To save changes, click **Apply**.

# Configuring quarantine settings in Kaspersky Endpoint Agent

This section describes how to configure the quarantine settings by means of Kaspersky Endpoint Agent Management plug-in.

## About Kaspersky Endpoint Agent quarantine

*Quarantine* is a special local repository on a device with Kaspersky Endpoint Agent installed which is intended for storing files that are probably infected by viruses or cannot be disinfected at the time when they are detected. Quarantined files are stored in an encrypted form and therefore do not compromise your device's security.

By default, the local quarantine is located in the `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<application version>\Quarantine` folder. By default, the objects restored from quarantine are stored in the `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\<application version>\Restored` folder.

Kaspersky Security Center generates a common list of quarantined objects on devices with Kaspersky Endpoint Agent installed. Network Agents on the devices submit information about quarantined files to the Administration Server.

Kaspersky Security Center does not copy files from quarantine to the Administration Server. All objects are stored on protected devices with Kaspersky Endpoint Agent installed. Objects are restored from the quarantine also on the protected devices.

## About quarantine management in Kaspersky Endpoint Agent

You can use the Kaspersky Security Center to configure quarantine settings, view the properties of the quarantined objects on the protected devices, initiate scanning of these objects, delete quarantined objects, and restore objects from Quarantine. For detailed information on managing the quarantined objects using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

> In order for Kaspersky Endpoint Agent to send data about quarantined objects to Kaspersky Security Center Administration Server, the corresponding option must be enabled in the quarantine settings in Kaspersky Endpoint Agent policy. This option is enabled by default.

Using the command line interface on the device, you can view information about quarantine settings and properties of the quarantined objects.

The object is quarantined with the permissions of the system account (SYSTEM).

Quarantined objects can be removed through the command line interface only with the permissions of the local account of the protected device user.

## Configuring quarantine settings and restoration of objects from quarantine

*To configure the quarantine settings:*

1. Open Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:
   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.
4. In the **Repositories** section select the **Quarantine** subsection.
5. In the **Quarantine settings** section configure the quarantine settings:
   a. In the **Quarantine folder** field, enter the path to where you want to create the Quarantine folder on the devices or click **Browse** and select the path.

      The default path is `%SOYUZAPPDATA%\Quarantine\`. The Quarantine folder is created on all devices with Kaspersky Endpoint Agent at the following path: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

      The value of the `%ALLUSERSPROFILE%` variable depends on the operating system of the device where Kaspersky Endpoint Agent is installed.

      Example:
      If the device has the Windows 7 operating system installed and Kaspersky Endpoint Agent is installed on drive C, the path to the Quarantine folder is:
      `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Quarantine`

   b. To configure the maximum quarantine size, select the **Maximum Quarantine size (MB)** check box and type the maximum size of quarantine in MB or select it from the list.

      For example, you can set the maximum quarantine size to 200 MB.

      When the maximum quarantine size is reached, Kaspersky Endpoint Agent publishes the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but does not stop quarantining new objects.

   c. To specify the quarantine threshold (the space in quarantine remaining until the maximum quarantine size is reached), select the **Threshold value for space available (MB)** check box.

      For example, you can set the quarantine threshold value to 50 MB.

      When the quarantine threshold is reached, Kaspersky Endpoint Agent publishes the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but does not stop quarantining new objects.

6. In the **Restoring objects from Quarantine** section, in the **Target folder for restored objects** field, specify the path to create the folder for objects restored from quarantine.

   The default path is `%SOYUZAPPDATA%\Restored\`. The Restored folder is created on all devices with Kaspersky Endpoint Agent at the following path: `%ALLUSERSPROFILE%\Kaspersky Lab\Endpoint Agent\4.0`.

   The value of the `%ALLUSERSPROFILE%` variable depends on the operating system of the device where Kaspersky Endpoint Agent is installed.

   Example:
   If the device has the Windows 7 operating system installed and Kaspersky Endpoint Agent is installed on drive C, the path to the folder with the objects restored from quarantine is:
   `C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

7. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

8. Click **Apply** and **OK**.

Quarantine settings and the folder for restoring objects from quarantine are configured.

### Configuring data synchronization with the Administration Server

You can configure synchronization of data on quarantined objects on managed devices with Kaspersky Security Center Administration Server.

*To configure data synchronization with the Administration Server:*

1. Open Kaspersky Security Center Administration Console.

2. In the console tree, open the **Policies** folder.

3. Select Kaspersky Endpoint Agent policy and open its properties window in one of the following ways:

   - Double-click the policy name.
   - Select **Properties** in the policy context menu.
   - Select the **Configure policy settings** item in the right part of the window.

4. In the **Repositories** section select the **Synchronization with Administration Server** subsection.

5. In the **Settings** section in the **Send the following data to Administration Server** subsection, select the **Data about objects, quarantined on managed hosts** check box.

6. In the upper right corner of the settings group, change the switch from **Policy not enforced** to **Under policy**.

7. Click **Apply** and **OK**.

Data synchronization with the Administration Server is configured.

## Managing Kaspersky Endpoint Agent tasks

This section describes how to manage Kaspersky Endpoint Agent tasks.

## Creating a local task

*To create a local task:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Managed devices** folder.
3. In the **Managed devices** folder, select the folder with the name of the administration group, which includes the required device.
4. In the workspace, select the **Devices** tab.
5. Select the device for which you want to create a local task.
6. Do one of the following:
   - In the context menu of the device, select **All tasks** → **Create a task**.
   - In the context menu of the device, select **Properties** and in the **Properties: <Device name>** window that opens on the **Tasks** tab, click **Add**.
   - In the **Perform action** drop-down list, select the **Create a task** item.

   The task creation wizard starts.
7. Select the required task and click **Next**.
8. Follow the instructions of the task creation wizard.

## Creating a group task

*To create a group task:*

1. Open Kaspersky Security Center Administration Console.
2. Do one of the following:
   - In the Administration Console tree, select the **Managed devices** folder to create a group task for all devices managed using Kaspersky Security Center.
   - In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required devices.
3. In the workspace, select the **Tasks** tab.
4. Click **Create a task**.

   The task creation wizard starts.

5. Select the required task and click **Next**.
6. Follow the instructions of the task creation wizard.

## Viewing the table of tasks

*To view the list of tasks on Kaspersky Security Center server:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

A list of task appears.

## Deleting a task from the list

*To remove tasks from the list of the tasks on Kaspersky Security Center server:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
3. In the task list, select the tasks that you want to delete and right-click them to open the context menu.
   A list of actions that you can perform on the tasks is displayed.
4. Select the **Delete** action.
   The action confirmation window opens.
5. Click **Yes**.

Selected tasks are deleted from the list.

## Starting the tasks manually

*To start a single task manually:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of task appears.
3. In the context menu of the desired task, select the **Run** action.

The task will run.

## Viewing task execution results

You can view the task execution results during their storage period. You can change the storage period for the task execution results.

It is not recommended to shorten the storage period for IOC Scan task execution results.

*To view the task execution results:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of task appears.
3. Select the task in the list and right-click it to open the task actions menu.
4. Select the **Results** menu item.

The **Task execution results** window opens.

## Configuring the storage time for the task execution results on the Administration Server

By default, task execution results are stored on the Administration Server for seven days.

*To configure storage time for the task execution results on the Administration Server:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of task appears.
3. Select the task in the list and right-click it to open the task actions menu.
4. Select the **Properties** menu item.

   The task properties window opens.
5. In the left part of the window, select the **Notification** section.
6. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section and specify for how many days you want to store the task execution results.
7. Click **Apply** and **OK**.

It is not recommended to shorten the storage period for IOC Scan task execution results.

# Managing Kaspersky Endpoint Agent activation tasks

You can activate Kaspersky Endpoint Agent using a key or activation code.

When activating the application using an activation code, data is sent to the activation server to verify the entered code.

> To activate the application using the activation code, the protected device must be connected to the Internet.

*To create Kaspersky Endpoint Agent activation task:*

1. Run the **Activation of Application** task creation wizard for the desired scope in one of the following ways:

   - **Start the local task creation wizard**.

     *To create a local task:*

     1. Open Kaspersky Security Center Administration Console.
     2. In Kaspersky Security Center Administration Console tree, open the **Managed devices** folder.
     3. In the **Managed devices** folder, select the folder with the name of the administration group, which includes the required device.
     4. In the workspace, select the **Devices** tab.
     5. Select the device for which you want to create a local task.
     6. Do one of the following:

        - In the context menu of the device, select **All tasks** → **Create a task**.
        - In the context menu of the device, select **Properties** and in the **Properties: <Device name>** window that opens on the **Tasks** tab, click **Add**.
        - In the **Perform action** drop-down list, select the **Create a task** item.

        The task creation wizard starts.

     7. Select the required task and click **Next**.
     8. Follow the instructions of the task creation wizard.

- **Start the group task creation wizard**.

  *To create a group task:*

  1. Open Kaspersky Security Center Administration Console.
  2. Do one of the following:
     - In the Administration Console tree, select the **Managed devices** folder to create a group task for all devices managed using Kaspersky Security Center.
     - In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required devices.
  3. In the workspace, select the **Tasks** tab.
  4. Click **Create a task**.

     The task creation wizard starts.
  5. Select the required task and click **Next**.
  6. Follow the instructions of the task creation wizard.

2. If you want to activate the application using an activation code, perform the following actions in the **Activation Settings** window:

   a. Select the **Activate with an activation code** option and click **Select**.

   b. In the window that opens, enter the activation code and click **OK**.

3. If you want to activate the application using a key file or a key from Kaspersky Security Center key storage, perform the following actions in the **Activation Settings** window:

   a. Select the **Activate with a key file or key** option and click **Select**.

   b. In the drop-down list, select the key distribution method.

   c. If you select the **Key file from folder** option, in the window that opens, specify the location of the key file and click **Open**.

   d. If you select the **Key from Kaspersky Security Center Storage** option, in the window that opens, select the key and click **OK**.

   For detailed information on Kaspersky Security Center key storage, refer to *Kaspersky Security Center Help*.

4. If you want to add an additional key to automatically renew the license, select the **Add this key as an additional** check box.

5. Click **Next**.

6. In the **Schedule** window, configure the task schedule settings and click **Next**.

   For detailed information on configuring the settings in this window, refer to Kaspersky Security Center Help.

7. In the **Selecting an account to run a task** window, specify the account to be used to run the task, and click **Next**.

   For detailed information on configuring the settings in this window, refer to Kaspersky Security Center Help.

8. In the **Define the task name** window, enter the name of the task and click **Next**.

9. If you want to run the task immediately after creation, select the **Run task after wizard finishes** check box.

10. Click **Finish**.

The application activation task is created for the selected device or device group.

# Managing Kaspersky Endpoint Agent database update tasks

You can create and the configure settings for the Database and application module update task.

## Creating Database and application module update task

*To create the Database and application module update task for Kaspersky Endpoint Agent in Kaspersky Security Center:*

1. Open Kaspersky Security Center Administration Console.

2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

3. Click **Create a task**.

   The task creation wizard starts.

4. Select **Kaspersky Endpoint Agent** application to create the task, and the **Database and application module update** task type.

5. Click **Next**.

   The Database Update task creation wizard starts.

The Database Update task creation wizard consists of the following steps:

1. **Selecting a database update source**

   Do the following:

   1. In the **Database update source** section, select one of the following database update sources:

      - **Kaspersky Security Center Administration Server**.
      - **Kaspersky update servers**.
      - **Custom HTTP or FTP servers or network folders**.

   2. If required, select the **Use Kaspersky update servers if specified servers are not available** check box.

3. If you select **Custom HTTP or FTP servers or network folders** as database update source, do the following:

   a. Click the **Custom HTTP or FTP servers or network folders** link.

   b. Add update servers to the list:

      1. Click **Update servers**.
      2. In the line that appears, enter the IP address of the update server.
      3. If you want to use this server to update databases, select the check box next to its IP address. You can also add servers to the list and clear the check boxes next to the IP addresses of servers that you do not want to use now, but plan to use later.

         Perform the same steps to add each server.

      4. Click **OK**.
      5. The **Update servers** window closes.

2. **Configuring the application modules update settings**

   Do the following:

   1. In the **Update settings** section, select the conditions for the application to check for the availability of application module updates:

      - **Do not check for available update**. Kaspersky Endpoint Agent will not check the availability of application module updates.
      - **Only check for available important software modules update**. Kaspersky Endpoint Agent will check the availability only for important application module updates.
      - **Download and install critical software modules update**. Kaspersky Endpoint Agent will check the availability of application module updates and download and install critical application module updates.

   2. If you want the application to display a notification about all scheduled application modules updates available in the update source, select the **Receive information about available scheduled software modules update** check box.

3. **Configuring database update schedule**

   Do the following:

   1. In the **Tasks schedule** section, select the **Run by schedule** check box.
   2. In the **Frequency** list select one of the following options to run the tasks: **At specified time**, **Every hour**, **Every day**, **every week**, **On application launch** or **After the application database update**.
   3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.

4. If you select one of the following options: **Every hour**, **Every day** or **every week**, configure the following settings in the **Run by schedule** section:

    a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.

    b. In the **Start time** and **Start date** lists, select the date and time from which the schedule applies.

5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:

    a. If you want to set maximum timeout for the task execution, select the **Quit task, running longer than** check box and specify the number of hours and minutes after which the task will automatically terminate.

    b. If you want the task schedule to be valid until a certain date, select the **Cancel schedule from** check box and specify the expiration date for the schedule.

    c. If you want the application to start Database Update tasks that were not completed on time as soon as possible, select the **Run missed tasks** check box.

    d. If you want to avoid simultaneous access of a large number of workstations to the Administration Server and run the task on workstations not according to the schedule, but randomly within a certain time interval, select the **Randomize the task run to every** check box and specify the start interval in minutes.

    e. Click **OK**.

6. Click **Next**.

4. **Selecting devices on which the task will be performed**

    In the device selection window that opens, select devices to which you want to assign the task and click **Next**.

    For example, you can select the **Assign task to an administration group** option and select an administration group from the list.

5. **Selecting Kaspersky Security Center user account which is used to run the task**

    In the **Selecting an account to run the task** window, do one of the following:

    - Select the default account and click **Next**.
    - Enter the user name and password to be used to start the task and click **Next**.

6. **Defining the task name**

    In the **Define the task name** window, enter the task name in the **Name** field, and click **Next**.

7. **Running the task immediately after it is created**

    If you want the task to start immediately after creation, select the **Run task after wizard finishes** check box and click **Finish**.

## Configuring Database and application module update task

You can configure the settings of the Database and application module update task after the task creation.

*To configure the task settings:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of task appears.
3. In the **Database and application module update** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.

   The task properties window opens.
5. In the left part of the window, select the group of settings that you want to configure.
6. In the right part of the window, make the necessary modifications and click **Apply** and **OK**.

You can configure the following task settings:

1. **Task name**

   Do the following:

   1. Select the **General** section.
   2. Change the task name in the top line.
2. **Devices on which the task will be performed**

   The right part of the window displays current devices to which the task is assigned. Perform the following actions to add devices:

   1. Click the **Add** button.

      A window opens with a list of managed devices.
   2. Select the check boxes next to devices you want to add.
   3. If you want to add devices that are not in the list, click **Add** in the right part of the window and follow the steps to add devices.

      For example, you can specify device addresses manually or import them from the list.

      You can specify NetBIOS names, DNS names, IP addresses and IP address ranges of the devices to which you want to assign a task.

   For details on working managed devices, refer to *Kaspersky Security Center Help*.

3. **Database update source**

   Do the following:

   1. In the **Database update source** section, select one of the following database update sources:

      - **Kaspersky Security Center Administration Server**.
      - **Kaspersky update servers**.
      - **Custom HTTP or FTP servers or network folders**.

   2. If required, select the **Use Kaspersky update servers if specified servers are not available** check box.

   3. If you select **Kaspersky update servers** as database update source and want to use a proxy-server to connect to it, select the **Use proxy server settings to connect to Kaspersky update servers** check box in the **Update source connection settings** section.

   4. If you select **Custom HTTP or FTP servers or network folders** as database update source, do the following:

      a. Click the **Custom HTTP or FTP servers or network folders** link.

      b. Add update servers to the list:

         1. Click **Update servers**.
         2. In the line that appears, enter the IP address of the update server.
         3. If you want to use this server to update databases, select the check box next to its IP address. You can also add servers to the list and clear the check boxes next to the IP addresses of servers that you do not want to use now, but plan to use later.

            Perform the same steps to add each server.

         4. Click **OK**.
         5. The **Update servers** window closes.

      c. To use a proxy server to connect to update servers, select the **Use proxy server settings to connect to other servers** check box in the **Update source connection settings** section.

4. **Configuring additional database update settings**

   Do the following:

   1. In the **Update settings** section, select the conditions for the application to check for the availability of application module updates:

      - **Do not check for available update**. Kaspersky Endpoint Agent will not check the availability of application module updates.
      - **Only check for available important software modules update**. Kaspersky Endpoint Agent will check the availability only for important application module updates.
      - **Download and install critical software modules update**. Kaspersky Endpoint Agent will check the availability of application module updates and download and install critical application module updates.

   2. If you want the application to display a notification about all scheduled application modules updates available in the update source, select the **Receive information about available scheduled software modules update** check box.

5. **Database update schedule**

   Do the following:

   1. In the **Task schedule** section, select the **Run by schedule** check box.
   2. In the **Frequency** list select one of the following options to run the tasks: **At specified time**, **Every hour**, **Every day**, **every week**, **On application launch** or **After the application database update**.
   3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
   4. If you select one of the following options: **Every hour**, **Every day** or **every week**, configure the following settings in the **Run by schedule** section:

      a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.

      b. In the **Start time** and **Start date** lists, select the date and time from which the schedule applies.

   5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:

      a. If you want to set maximum timeout for the task execution, select the **Quit task, running longer than** check box and specify the number of hours and minutes after which the task will automatically terminate.

      b. If you want the task schedule to be valid until a certain date, select the **Cancel schedule from** check box and specify the expiration date for the schedule.

      c. If you want the application to start Database Update tasks that were not completed on time as soon as possible, select the **Run missed tasks** check box.

      d. If you want to avoid simultaneous access of a large number of workstations to the Administration Server and run the task on workstations not according to the schedule, but randomly within a certain time interval, select the **Randomize the task run to every** check box and specify the start interval in minutes.

      e. Click **OK**.

6. **Kaspersky Security Center user account which is used to run the task**

   In the **Selecting an account to run the task** window, do one of the following:

   - Select the default account and click **Next**.
   - Enter the user name and password to be used to start the task.

7. **Storage time for the task execution results on the Administration Server**

   Do the following:

   1. Select the **Notification** section.
   2. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section, and specify for how many days you want to store the task execution results.

      By default, task execution results are stored on the Administration Server for 7 days.

# Managing IOC Scan tasks in Kaspersky Endpoint Agent

This section describes how to manage IOC Scan tasks in Kaspersky Endpoint Agent using Kaspersky Endpoint Agent Management plugin.

## About IOC Scan tasks in Kaspersky Endpoint Agent

While executing IOC Scan tasks Kaspersky Endpoint Agent uses IOC files (indicators of compromise files of the OpenIOC open description standard) to search for these indicators on devices.

Kaspersky Endpoint Agent supports three types of IOC Scan tasks:

- *Standard IOC Scan tasks* are created manually in Kaspersky Security Center or through the command line interface.
- *Autonomous IOC Scan tasks* are created automatically in response to the threats detected by Kaspersky Anti Targeted Attack Platform.
- *IOC scan by IOC files downloaded manually via Kaspersky Anti Targeted Attack Platform web interface* allows application users to use IOC files to search for signs of targeted attacks, infected and probably infected objects in the event and detection database, and to scan computers with Kaspersky Endpoint Agent installed.

Different tasks are managed in different ways, have different configurable settings, and different task scopes. Description of each type of IOC Scan task is provided in the table below.

IOC Scan task types

| Task type | Task description | Task scope |
|---|---|---|
| Standard IOC Scan tasks | These tasks are created and configured manually in Kaspersky Security Center or through the command line interface, without integration with third-party systems.<br><br>IOC files prepared by the user are used to run the tasks.<br><br>Task settings do not depend on the policies.<br><br>You can specify the following actions to respond to the detected IOCs (not available when running the tasks from the command line):<br><br>• Run on-demand scan tasks using EPP on the device.<br>• Enable network isolation of the device.<br>Viewing reports is available both in the task execution results as a summary table and in the Detected IOCs card. | Local or group |
| Autonomous IOC Scan tasks | These tasks are created automatically if in Kaspersky Endpoint Agent policy, the **Run IOC scanning on a managed group of hosts** action is selected in response to the threats detected by Kaspersky Sandbox.<br><br>Kaspersky Endpoint Agent generates an IOC file automatically. Operations with custom IOC files are not supported.<br><br>Limited task management in Kaspersky Security Center is available for the user.<br><br>In the policy settings you can specify the task start schedule and the scan area for the task.<br><br>Tasks are automatically deleted in seven days after the last start or after creation if tasks were never started.<br><br>You can specify the following actions to respond to the detected IOCs:<br><br>• Run on-demand scan tasks using EPP on the device.<br>• Quarantine the object and delete it from the device.<br>Viewing reports is available both in the task execution results as a summary table and in the Detected IOCs card. | Group |
| IOC Scan by IOC files downloaded manually via Kaspersky Anti Targeted Attack Platform web interface | IOC files are downloaded manually via Kaspersky Anti Targeted Attack Platform web interface. It is also possible to configure IOC scan schedule for computers with Kaspersky Endpoint Agent in the web interface of Kaspersky Anti Targeted Attack Platform.<br><br>Task management in Kaspersky Security Center or through the command line is not supported.<br><br>No actions are automatically performed when IOC is detected.<br><br>Task settings do not depend on Kaspersky Endpoint Agent policies. | Not applicable |

The results of group IOC Scan tasks execution can be viewed in Kaspersky Security Center within 7 days since the task execution completed, or until the task is removed.

# Managing IOC Scan tasks in Kaspersky Endpoint Agent

You can manage IOC Scan tasks in Kaspersky Security Center or through Kaspersky Endpoint Agent command line interface, as well as download IOC files and configure IOC scan schedule in Kaspersky Anti Targeted Attack Platform web interface. The description of each IOC Scan task type and information on the available management capabilities for IOC Scan tasks are shown in the table below.

Managing IOC Scan tasks.

| Task type | Using Kaspersky Security Center | Using the Central Node component | Using the command line interface |
|---|---|---|---|
| Standard IOC Scan task | • Creating, removing and starting the task manually.<br>• Viewing detailed reports on the task execution results as a summary table and in the Detected IOCs card.<br>• IOC collection export.<br>• Configuring the following task settings in the task creation wizard or in the task properties after the task creation:<br>  • IOC collection settings.<br>  • IOC scan settings.<br>  • Application actions when detecting IOC (network isolation of the device and start of the scan tasks using EPP on the device).<br>  • Task schedule settings.<br>  • Storage time for the task execution results on the Administration Server (unavailable in the task creation wizard). | Task management is not applicable. | • Creating and running the task with the required settings.<br>• Viewing data on the task execution. |
| Autonomous IOC Scan task | • Configuring the task start settings.<br>• Starting and removing the task manually.<br>• Enabling response to the threats detected by Kaspersky Sandbox.<br>• Adding an action to automatically create an Autonomous IOC Scan Task.<br>• Viewing detailed reports on the task execution results as a summary table and in the Detected IOCs card.<br>• IOC collection export.<br>• Configuring the following settings in the task properties:<br>  • Application actions when detecting IOC (quarantining an object and deleting it from the device; starting the scan tasks using EPP on the device).<br>  • Task schedule settings.<br>  • Storage time for the task execution results on the Administration Server. | Task management is not applicable. | Task management is not applicable. |
| IOC Scan task created by Central Node | Task management is not applicable. | Downloading IOC files, configuring IOC scan schedule. | Task management is not applicable. |

# Managing Standard IOC Scan tasks

*Standard IOC Scan tasks* are created manually in Kaspersky Security Center or through the command line interface.

This section describes how to manage Standard IOC Scan tasks using Kaspersky Endpoint Agent Management plugin.

## Requirements for IOC files

Kaspersky Endpoint Agent supports IOC files with the ioc and xml extensions. These files use open standard for IOC description – OpenIOC versions 1.0 and 1.1.

If, when creating the IOC Scan task, you upload some IOC files that are not supported by Kaspersky Endpoint Agent then when the task starts, the application will use only supported IOC files.

If, when creating the IOC Scan task, none of the downloaded IOC files is supported by Kaspersky Endpoint Agent, the task can be started, but as a result of the task execution, no indicators of compromise will be detected.

Semantic errors and IOC terms and tags in IOC files that are not supported by the application do not cause the task execution errors. The application just does not detect matches in such sections of IOC files.

Identifiers of all IOC files that are used in the same IOC Scan task must be unique. The presence of IOC files with the same identifier can affect the correctness of the task execution results.

Features and limitations of the OpenIOC standard support by the application are listed in the following table.

Features and limitations of the OpenIOC versions 1.0 and 1.1 standard support.

| | |
|---|---|
| Supported conditions | OpenIOC 1.0:<br><br>`is`<br>`isnot` (as an exclusion from the set)<br>`contains`<br>`containsnot` (as an exclusion from the set)<br>OpenIOC 1.1:<br><br>`is`<br>`contains`<br>`starts-with`<br>`ends-with`<br>`matches`<br>`greater-than`<br>`less-than` |
| Supported condition attributes | OpenIOC 1.1:<br><br>`preserve-case`<br>`negate` |
| Supported operators | `AND`<br>`OR` |
| Supported data types | `date`: date (applicable conditions: `is`, `greater-than`, `less-than`)<br><br>`int`: integer number (applicable conditions: `is`, `greater-than`, `less-than`)<br><br>`string`: string (applicable conditions: `is`, `contains`, `matches`, `starts-with`, `ends-with`)<br><br>`duration`: duration in seconds (applicable conditions: `is`, `greater-than`, `less-than`) |

| | |
|---|---|
| Data types interpretation details | The following data types are interpreted as string: `Boolean string`, `restricted string`, `md5`, `IP`, `sha256`, `base64Binary`.<br><br>The application supports interpretation of the `Content` parameter specified as intervals for the following data types: `int` and `date`:<br><br>OpenIOC 1.0:<br>Using the `TO` operator in the `Content` field:<br>`<Content type="int">49600 TO 50700</Content>`<br>`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`<br>`<Content type="int">[154192 TO 154192]</Content>`<br>OpenIOC 1.1:<br>Using the `greater-than` and `less-than` conditions<br>Using the `TO` operator in the `Content` field<br>The application supports interpretation of the `date` and `duration` data types if the indicators are specified in the `ISO 8601, Zulu time zone, UTC` format. |
| Supported IOC terms | The full list of supported IOC terms is provided in a separate table. |

## Supported IOC terms

The file that can be downloaded by the following link contains a table with a full list of supported IOC terms of the OpenIOC standard.

DOWNLOAD IOC_TERMS.XLSX FILE

## Creating and configuring Standard IOC Scan task

*To create and configure a Standard IOC Scan task,*

depending on the required task scope, perform one of the following actions:

- **Start the local task creation wizard**.

  *To create a local task:*

  1. Open Kaspersky Security Center Administration Console.
  2. In Kaspersky Security Center Administration Console tree, open the **Managed devices** folder.
  3. In the **Managed devices** folder, select the folder with the name of the administration group, which includes the required device.
  4. In the workspace, select the **Devices** tab.
  5. Select the device for which you want to create a local task.
  6. Do one of the following:

     - In the context menu of the device, select **All tasks** → **Create a task**.
     - In the context menu of the device, select **Properties** and in the **Properties: <Device name>** window that opens on the **Tasks** tab, click **Add**.
     - In the **Perform action** drop-down list, select the **Create a task** item.

  The task creation wizard starts.

7. Select the required task and click **Next**.
8. Follow the instructions of the task creation wizard.

- **Start the group task creation wizard**.

  *To create a group task:*

  1. Open Kaspersky Security Center Administration Console.
  2. Do one of the following:
     - In the Administration Console tree, select the **Managed devices** folder to create a group task for all devices managed using Kaspersky Security Center.
     - In the **Managed devices** folder of the Administration Console tree, select the folder with the name of the administration group, which includes the required devices.
  3. In the workspace, select the **Tasks** tab.
  4. Click **Create a task**.

     The task creation wizard starts.
  5. Select the required task and click **Next**.
  6. Follow the instructions of the task creation wizard.

The task creation wizard allows you to configure the following settings:

- **IOC collection**

  *To configure IOC collection:*

  1. In the **IOC collection** group of settings click **Browse**.
  2. In the context menu, do one of the following:
     - Select the **Browse for folder** item to add a group of IOC files to the IOC collection.
     - Select the **Browse for file** item to add one IOC file to the IOC collection.
  3. Depending on your choice, do one of the following in the window that opens:
     - Specify the path to the folder with IOC files and click **OK**.
     - Specify the path to IOC file and click **Open**.

     If, when creating the IOC Scan task, you upload some IOC files that are not supported by Kaspersky Endpoint Agent then when the task starts, the application will use only supported IOC files.
  4. To view the list of all IOC files that are included in the IOC collection, as well as information about each IOC file, click **View**.

     The **Browse for folder** window opens. In this window, you can exclude any file from the database by clearing the check box next to the name of the IOC file.

5. Click **OK** to save the changes and close the **Browse for folder** window.

6. To export the created IOC collection, click **Export**.

   In the window that opens, specify the name of the file and select the folder where you want to save it.

7. Click the **Save** button.

   The application creates a ZIP file in the specified folder.

- **Data types (IOC documents) to be analyzed during IOC scan**

  *To configure IOC terms and IOC documents to be used to search for IOCs:*

  1. Click the **Configure IOC terms and documents** button.

     The data type configuration window opens.

  2. Select the IOC terms and IOC documents that you want to analyze during the execution of the IOC Scan task.

  Selection of the data types to be analyzed (IOC terms and IOC documents) for the IOC Scan task is mandatory.

- **Application actions on IOC detection**

  *To configure Kaspersky Endpoint Agent actions on IOC detection:*

  1. In the **Actions** section, select the **Take response actions when an Indicator of Compromise is detected** check box.

  2. Select the **Isolate device from the network** check box to enable network isolation of the device on which indicator of compromise is detected by Kaspersky Endpoint Agent.

  3. Select the **Push Endpoint Protection Platform (EPP) scanning on critical areas** check box so that Kaspersky Endpoint Agent sends a command to EPP application to scan critical areas on all the devices of the administration group on which indicators of compromise are detected.

- **Task start schedule**

  *To configure the schedule settings for IOC Scan task:*

  1. In the **Task schedule** section, select the **Run by schedule** check box.

  2. In the **Frequency** list select one of the following options to run IOC Scan tasks: **At specified time**, **Every hour**, **Every day**, **every week** or **On application launch**.

  3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.

  4. If you select one of the following options: **Every hour**, **Every day** or **every week**, configure the following settings in the **Run by schedule** section:

     a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.

     b. In the **Start time** and **Start date** lists, select the date and time from which the schedule applies.

5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:

   a. If you want to set maximum timeout for the task execution, select the **Quit task, running longer than** check box and specify the number of hours and minutes after which the task will automatically terminate.

   b. If you want the task schedule to be valid until a certain date, select the **Cancel schedule from** check box and specify the expiration date for the schedule.

   c. If you want the application to start IOC Scan tasks that were not completed on time as soon as possible, select the **Run missed tasks** check box.

   d. If you want to avoid simultaneous access of a large number of workstations to the Administration Server and run the task on workstations not according to the schedule, but randomly within a certain time interval, select the **Randomize the task run to every** check box and specify the start interval in minutes.

   e. Click **OK**.

- **Kaspersky Security Center user account to run the task**

  *To select Kaspersky Security Center user account, under which you want to run the task,*

  perform one of the following actions in the group of settings for selecting account to start the task:

  - Select the default account and click **Next**.
  - Enter the name and password of the user, whose account permissions will be used to start the task.

- **Task name**

  The task name cannot be longer than 100 characters long and cannot contain special characters ("* <>? \: |).

Identifiers of all IOC files that are used in the same IOC Scan task must be unique. The presence of IOC files with the same identifier can affect the correctness of the task execution results.

If, when creating the IOC Scan task, you upload some IOC files that are not supported by Kaspersky Endpoint Agent then when the task starts, the application will use only supported IOC files.

Semantic errors and IOC terms and tags in IOC files that are not supported by the application do not cause the task execution errors. The application just does not detect matches in such sections of IOC files.

## Configuring Standard IOC Scan task

*To configure the settings of a Standard IOC Scan task:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   The list of tasks is displayed in the workspace.
3. Open the settings of the required task in one of the following ways:
   - Double-click the task name.
   - Open the policy context menu and select **Properties**.
   - Select a task and click **Configure task** in the right part of the window.

   The **Properties: <Task name>** window opens.
4. In the left part of the window, select the group of settings that you want to configure.
5. In the right part of the window, make the necessary modifications and click **Apply** and **OK**.

You can configure the following task settings:

- **Task name**

  Do the following:

  1. Select the **General** section.
  2. Change the task name in the top line.

- **Storage time for the task execution results on the Administration Server**

  Do the following:

  1. Select the **Notification** section.
  2. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section, and specify for how many days you want to store the task execution results.

     By default, task execution results are stored on the Administration Server for 7 days.

- **IOC collection**

  *To configure IOC collection:*

  1. In the **IOC collection** group of settings click **Browse**.
  2. In the context menu, do one of the following:
     - Select the **Browse for folder** item to add a group of IOC files to the IOC collection.
     - Select the **Browse for file** item to add one IOC file to the IOC collection.
  3. Depending on your choice, do one of the following in the window that opens:
     - Specify the path to the folder with IOC files and click **OK**.
     - Specify the path to IOC file and click **Open**.

     If, when creating the IOC Scan task, you upload some IOC files that are not supported by Kaspersky Endpoint Agent then when the task starts, the application will use only supported IOC files.
  4. To view the list of all IOC files that are included in the IOC collection, as well as information about each IOC file, click **View**.

     The **Browse for folder** window opens. In this window, you can exclude any file from the database by clearing the check box next to the name of the IOC file.
  5. Click **OK** to save the changes and close the **Browse for folder** window.
  6. To export the created IOC collection, click **Export**.

     In the window that opens, specify the name of the file and select the folder where you want to save it.
  7. Click the **Save** button.

     The application creates a ZIP file in the specified folder.

- **Application actions on IOC detection**

  *To configure Kaspersky Endpoint Agent actions on IOC detection:*

  1. In the **Actions** section, select the **Take response actions when an Indicator of Compromise is detected** check box.
  2. Select the **Isolate device from the network** check box to enable network isolation of the device on which indicator of compromise is detected by Kaspersky Endpoint Agent.
  3. Select the **Push Endpoint Protection Platform (EPP) scanning on critical areas** check box so that Kaspersky Endpoint Agent sends a command to EPP application to scan critical areas on all the devices of the administration group on which indicators of compromise are detected.

- **Data types (IOC documents) to be analyzed during IOC scan**

  *To select data types (IOC documents) that you want to analyze during IOC scan:*

  1. Select the **Advanced** section.
  2. Select the IOC terms and IOC documents that you want to analyze during the execution of the IOC Scan task.

  Selection of the data types to be analyzed (IOC terms and IOC documents) for the IOC Scan task is mandatory.

- **IOC Scan task schedule**

  *To configure the schedule settings for IOC Scan task:*

  1. In the **Task schedule** section, select the **Run by schedule** check box.
  2. In the **Frequency** list select one of the following options to run IOC Scan tasks: **At specified time**, **Every hour**, **Every day**, **every week** or **On application launch**.
  3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.
  4. If you select one of the following options: **Every hour**, **Every day** or **every week**, configure the following settings in the **Run by schedule** section:
     a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.
     b. In the **Start time** and **Start date** lists, select the date and time from which the schedule applies.
  5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:
     a. If you want to set maximum timeout for the task execution, select the **Quit task, running longer than** check box and specify the number of hours and minutes after which the task will automatically terminate.
     b. If you want the task schedule to be valid until a certain date, select the **Cancel schedule from** check box and specify the expiration date for the schedule.
     c. If you want the application to start IOC Scan tasks that were not completed on time as soon as possible, select the **Run missed tasks** check box.
     d. If you want to avoid simultaneous access of a large number of workstations to the Administration Server and run the task on workstations not according to the schedule, but randomly within a certain time interval, select the **Randomize the task run to every** check box and specify the start interval in minutes.
     e. Click **OK**.

- **Kaspersky Security Center user account to run the task**

  *To select Kaspersky Security Center user account, under which you want to run the task,*

  perform one of the following actions in the group of settings for selecting account to start the task:

  - Select the default account and click **Next**.
  - Enter the name and password of the user, whose account permissions will be used to start the task.

- **Excluding groups of devices from the task scope**

  To exclude groups of devised from the task scope, in the **Exclusions from task scope** section, select the groups of devices to which the task will not be applied.

  Only the subgroups of the administration group to which the task applies can be excluded.

## IOC collection export

*To export an IOC collection:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of task appears.
3. In the **Run IOC Scan** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.
   The task properties window opens.
5. Select the **IOC Scan settings** section.
6. In the **IOC collection** section click **Export**.
7. In the window that opens, specify the name of the file and select the folder where you want to save it.
8. Click the **Save** button.
   The application creates a ZIP file in the folder you specified.

## Viewing IOC Scan task execution results

*To view the IOC Scan task execution results:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   The list of tasks is displayed in the workspace.

3. Open the settings of the required task in one of the following ways:

   - Double-click the task name.
   - Open the policy context menu and select **Properties**.
   - Select a task and click **Configure task** in the right part of the window.

   The **Properties: <Task name>** window opens.

4. Select the **Results** section.
5. In the **Show task results for the device** list, select the devices for which you want to view the results of IOC Scan tasks.
6. To view detailed information about a particular task, double-click it.
7. To view detailed information about the detected indicator of compromise, click the **Show detections card** button.

   *Detected IOCs card* contains information about objects that match the conditions of the processed IOC file, as well as the text of the matched branches or individual conditions from this IOC file.

   > Viewing the Detected IOCs card is not available for IOC files, for which no indicators of compromise were detected during scan.

# Managing Autonomous IOC Scan tasks

*Autonomous IOC Scan tasks* are created automatically in response to the threats detected by Kaspersky Anti Targeted Attack Platform.

This section describes how to configure the settings of Autonomous IOC Scan tasks using Kaspersky Endpoint Agent Management plug-in.

## About Autonomous IOC Scan tasks

*Autonomous IOC Scan tasks* are created automatically on Kaspersky Security Center server if the **Run IOC scanning on a managed group of hosts** action is configured in Kaspersky Endpoint Agent policies in response to threats.

> Manual creation of Autonomous IOC Scan tasks is not available.

You can view the list of tasks, remove unused tasks from the list, view task execution results, run the tasks manually, configure storage period for the task results, and configure IOC Scan task run settings.

> Automatically created tasks are stored on Kaspersky Security Center server. It is recommended that Kaspersky Endpoint Agent administrator makes sure that the number of tasks in the list is not more than 1000, and periodically manually removes the tasks from the list.

By default, Autonomous IOC Scan tasks are stored on Kaspersky Security Center server for seven days since the last start.

Kaspersky Endpoint Agent deletes Autonomous IOC Scan tasks if the application has been running without interruption for at least seven days on at least one device and one of the following conditions is met:

- The task was last running at least seven days ago.
- The task has never been started, and it was created at least seven days ago.

Kaspersky Endpoint Agent deletes an Autonomous IOC Scan task regardless of the device where the object was first detected and the action that was performed as a response to threats. The deleted task will not be available for all devices in the administration group.

Deletion of unused Autonomous IOC Scan tasks occurs automatically. The application does not provide the capability to configure settings for automatic deletion of Autonomous IOC Scan tasks.

If deletion of the Autonomous IOC Scan tasks was not performed correctly or you want to change the behavior of the application, contact Kaspersky Technical Support.

By default, the Autonomous IOC Scan task is configured to store all types of events that occur during execution of the group tasks. By default, execution results of the Autonomous IOC Scan tasks are stored for seven days. You can change the storage period for the task execution results.

It is not recommended to change the default storage settings for task execution results and to shorten the storage period for the Autonomous IOC Scan task execution results.

## Configuring user permissions to manage IOC Scan tasks

You need to configure Kaspersky Security Center user permissions, whose account will be used to manage IOC Scan tasks.

*To configure Kaspersky Security Center user permissions to managing IOC Scan tasks:*

1. Open Kaspersky Security Center Administration Console.
2. Select **Administration Server**.
3. In the Administration Server context menu, select **Properties**.

   The property window for the Administration Server.
4. In the left part of the window, select the **Security** section.
5. Select Kaspersky Security Center user, whose account will be used to manage IOC Scan tasks.

   At the bottom of the window, the list of the selected user permissions is displayed, grouped by the applications that the user can manage using Kaspersky Security Center.
6. In the **Kaspersky Endpoint Agent** group of permissions expand the **Intrusion Prevention** section.

7. Select the check boxes in the **Allow** column for the following types of permissions: **Modify**, **Execute**, and **Perform actions on device selections**.

8. Click **Apply** and **OK**.

## Configuring Autonomous IOC Scan task

*To configure settings of an Autonomous IOC Scan task:*

1. Open Kaspersky Security Center Administration Console.

2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of task appears.

3. In the **Run IOC Scan** section, select the task in the list and right-click it to open the task action menu.

4. Select the **Properties** menu item.

   The task properties window opens.

5. In the left part of the window, select the group of settings that you want to change.

6. In the right part of the window, make the necessary modifications and click **Apply** and **OK**.

You can configure the following task settings:

- **Task name**

  Do the following:

  1. Select the **General** section.

  2. Change the task name in the top line.

- **Storage time for the task execution results on the Administration Server**

  Do the following:

  1. Select the **Notification** section.

  2. Make sure, that the **On the Administration Server for (days)** check box is selected in the **Save information about results** section, and specify for how many days you want to store the task execution results.

     By default, task execution results are stored on the Administration Server for 7 days.

- **Application actions on IOC detection**

  *To configure the application actions on IOC detection:*

  1. Select the **IOC scanning settings** section.

  2. In the **Actions** group of settings, select the **Take response actions when an Indicator of Compromise is detected** check box.

3. Select the **Quarantine and delete** check box to quarantine the detected object and remove it from the device.

4. Select the **Push Endpoint Protection Platform (EPP) scanning on critical areas** check box so that Kaspersky Endpoint Agent sends a command to EPP application to scan critical areas on all the devices of the administration group on which the object is detected.

5. Click the **Apply** button.

- **IOC Scan task schedule**

  *To configure the schedule settings for IOC Scan task:*

  1. In the **Task schedule** section, select the **Run by schedule** check box.

  2. In the **Frequency** list select one of the following options to run IOC Scan tasks: **At specified time**, **Every hour**, **Every day**, **every week** or **On application launch**.

  3. If you select the **At specified time** option, specify the day and time to start the task in the **Run by schedule** section.

  4. If you select one of the following options: **Every hour**, **Every day** or **every week**, configure the following settings in the **Run by schedule** section:

     a. In the **Every** list, select the task run frequency. For example, once a day or twice a week on Tuesdays and Thursdays.

     b. In the **Start time** and **Start date** lists, select the date and time from which the schedule applies.

  5. To configure advanced schedule settings, click the **Advanced** button and perform the following actions in the **Advanced** window:

     a. If you want to set maximum timeout for the task execution, select the **Quit task, running longer than** check box and specify the number of hours and minutes after which the task will automatically terminate.

     b. If you want the task schedule to be valid until a certain date, select the **Cancel schedule from** check box and specify the expiration date for the schedule.

     c. If you want the application to start IOC Scan tasks that were not completed on time as soon as possible, select the **Run missed tasks** check box.

     d. If you want to avoid simultaneous access of a large number of workstations to the Administration Server and run the task on workstations not according to the schedule, but randomly within a certain time interval, select the **Randomize the task run to every** check box and specify the start interval in minutes.

     e. Click **OK**.

- **Kaspersky Security Center user account to run the task**

  *To select Kaspersky Security Center user account, under which you want to run the task,*

  perform one of the following actions in the group of settings for selecting account to start the task:

  - Select the default account and click **Next**.

  - Enter the name and password of the user, whose account permissions will be used to start the task.

- **Excluding groups of devices from the task scope**

  To exclude groups of devised from the task scope, in the **Exclusions from task scope** section, select the groups of devices to which the task will not be applied.

  Only the subgroups of the administration group to which the task applies can be excluded.

## IOC collection export

*To export an IOC collection:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of task appears.
3. In the **Run IOC Scan** section, select the task in the list and right-click it to open the task action menu.
4. Select the **Properties** menu item.
   The task properties window opens.
5. Select the **IOC Scan settings** section.
6. In the **IOC collection** section click **Export**.
7. In the window that opens, specify the name of the file and select the folder where you want to save it.
8. Click the **Save** button.
   The application creates a ZIP file in the folder you specified.

## Viewing IOC Scan task execution results

*To view the IOC Scan task execution results:*

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   The list of tasks is displayed in the workspace.
3. Open the settings of the required task in one of the following ways:
   - Double-click the task name.
   - Open the policy context menu and select **Properties**.
   - Select a task and click **Configure task** in the right part of the window.

   The **Properties: <Task name>** window opens.
4. Select the **Results** section.

5. In the **Show task results for the device** list, select the devices for which you want to view the results of IOC Scan tasks.

6. To view detailed information about a particular task, double-click it.

7. To view detailed information about the detected indicator of compromise, click the **Show detections card** button.

   *Detected IOCs card* contains information about objects that match the conditions of the processed IOC file, as well as the text of the matched branches or individual conditions from this IOC file.

   Viewing the Detected IOCs card is not available for IOC files, for which no indicators of compromise were detected during scan.

# Managing Kaspersky Endpoint Agent through command line interface

Kaspersky Endpoint Agent can be managed through the command line interface. The functionality of the command line interface is provided by the Agent.exe utility. The Agent.exe utility is included in Kaspersky Endpoint Agent distribution kit and is installed on each device together with Kaspersky Endpoint Agent. It is installed to the `%ProgramFiles%\Kaspersky Lab\Endpoint Agent` folder (if 32-bit operating system is used on the device) or to the `% ProgramFiles(x86)%\Kaspersky Lab\Endpoint Agent` folder (if 64-bit operating system is used on the device).

Example:
If the device has x64 Windows operating system installed and you select to install Kaspersky Endpoint Agent on drive C, the Agent.exe utility is placed to the following folder:
`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`

*To manage Kaspersky Endpoint Agent through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Type the following command: `agent.exe --<application setting you want to configure>=<action on the setting you want to execute>` and press **ENTER**.

   The command execution result (return code) is displayed.

You can manage the following Kaspersky Endpoint Agent settings:

- `help`

  Displays help information on the application settings and their possible values.

- `trace`

  Allows you to configure tracing in Kaspersky Endpoint Agent.

  Available actions: `enable`, `disable`, `show`.

- `dump`

  Allows you to configure creation of dump files in Kaspersky Endpoint Agent.

  Available actions: `enable`, `disable`, `show`.

- `quarantine`

  Allows you to work with quarantine in Kaspersky Endpoint Agent.

  Available actions: `add`, `delete`, `restore`, `show`, `limits`.

- `sandbox`

  Allows you to manage Kaspersky Endpoint Agent integration with Kaspersky Sandbox.

  Available actions: `enable`, `disable`, `show`.

- `update`

  Allows you to manage Kaspersky Endpoint Agent database updates.

  Available actions: `bases`, `modules`.

- `ppl`

  Allows you to manage Kaspersky Endpoint Agent processes that are run with the PPL flag (these processes are protected by the Protected Process Light technology).

  Processes that are running with the PPL flag cannot be stopped or changed by other processes without the PPL flag.

  Usage of the PPL flag for the application services allows you to protect the services from malicious external influences and attempts to compromise the application.

  Available actions: `enable`, `disable`, `show`.

- `password`

  Allows you to manage password protection of Kaspersky Endpoint Agent.

  Available actions: `set`, `reset`, `state`.

- `product`

  Allows you to manage Kaspersky Endpoint Agent.

  Available actions: `start`, `stop`, `state`.

  Example:
  To display help on all the application settings and their possible values, run the following command:
  ```
  agent.exe --help
  ```

  To enable integration with Kaspersky Sandbox, run the following command:

  ```
  agent.exe --sandbox=enable
  ```

# Managing Kaspersky Endpoint Agent activation

*To manage application activation settings through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:

   - To activate the application using the activation code or key file:

     `agent.exe --license=add <activation code or path to the key file>`

     > To activate the application using the activation code, the protected device must be connected to the Internet.

   - To specify an additional key to automatically renew the license:

     `agent.exe --license=reserve <activation code or path to the key file>`

   - To remove the added primary or additional key:

     `agent.exe --license=delete <key serial number>`

   - To view the status of added keys:

     `agent.exe --license=show`

Return codes of the `--license` command:

- `E_EXPIRED` – the added key has expired.
- `E_FAIL` – undefined application error.
- `E_KEY_IN_BLST` – the added key is in the black list.
- `E_KEY_NOT_MATCH` – the added key is not suitable for Kaspersky Endpoint Agent activation.
- `E_GENERAL_ERROR` – general error (for example, key file is damaged).
- `E_INVALID_SYNTAX` – syntax errors.
- `E_INVALID_PATH` – invalid path to the key file is specified.

# Configuring tracing

*To configure tracing in Kaspersky Endpoint Agent through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --trace=enable --folder <path to the folder where you want to create trace files>` to enable tracing.

   Tracing will be enabled for all Kaspersky Endpoint Agent processes that are currently running. Trace files will be created in the folder you specified.

   - `agent.exe --trace=disable` to disable tracing.

   Tracing will be disabled for all Kaspersky Endpoint Agent processes that are currently running.

   - `agent.exe --trace=show` to view the current tracing status and the path to the folder to save the trace files.

   The values of the `trace.enable` (`true`, if tracing is enabled or `false`, is tracing is disabled) and `trace.folder` (path to the folder) settings are displayed.

Return codes of the `--trace` command:

- -1 – the command is not supported.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 5 – object not found (the specified path to the tracing logs folder is not found).
- 9 – invalid operation (for example, an attempt to execute the `--trace=disable` command, if tracing is already disabled).

# Configuring creation of dump files

*To configure creation of dump files in Kaspersky Endpoint Agent through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --dump=enable --folder <path to the folder where you want to create dump files>` to enable creation of dump files.

   Creation of dump files will be enabled for all Kaspersky Endpoint Agent processes that are currently running. Dump files will be created in the folder you specified.

   - `agent.exe --dump=disable` to disable dump creation.

   Creation of dump files will be disabled for all Kaspersky Endpoint Agent processes that are currently running.

   - `agent.exe --dump=show` to view the current dump creation status and the path to the folder with the dump files.

   The values of the `dump.enable` (`true`, if creation of dump files is enabled or `false`, if creation of dump files is disabled) and `dump.folder` (path to the folder) settings are displayed.

Return codes of the `--dump` command:

- -1 – the command is not supported.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 5 – object not found (could not find the specified path to the dump files folder).
- 9 – invalid operation (for example, an attempt to execute the `--dump=disable` command, if creation of dumps is already disabled).

# Viewing information about quarantine settings and quarantined objects

*To view information about the quarantine settings and quarantined objects through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --quarantine=show [--pwd=<current user password>]`, to view a list of quarantined objects.

   The following information will be displayed on all objects in the Quarantine folder on the devices (the Quarantine folder is specified when quarantine settings are configured):

   - Identifiers of objects quarantined by the current moment (`ouid` parameter).
   - Names of quarantined objects (name + extension).
   - Date and time when the object was quarantined (UTC).
   - Original path to the quarantined file and default path for restoring the quarantined file (without file name).
   - Size of quarantined file (in bytes).
   - User account whose permissions were used to run the task for quarantining the file.
   - Object status:
     - `DETECT` if the file was quarantined by EPP or while performing actions in response to a threat detected by Kaspersky Sandbox. For example, as a result of the **Quarantine and delete** local action or the **Quarantine and delete when IOC is detected** global action.
     - `CUSTOM` if the file was quarantined manually, as a result of the `--quarantine=add` command execution.

- The way the file was quarantined:
  - `AUTOMATIC_<name of the application that detected a threat in the quarantined file>`, if the file was quarantined by EPP or while performing actions in response to a threat detected by Kaspersky Sandbox. For example, as a result of the **Quarantine and delete** local action or the **Quarantine and delete when IOC is detected** global action.
  - `BY USER` if the file was quarantined manually, as a result of the `--quarantine=add` command execution.
- `agent.exe --quarantine=limits`, to view the current values of the **Maximum Quarantine size (MB)** and **Threshold value for space available (MB)** settings, as well as the statuses of applying these settings (check box statuses) specified when configuring the quarantine.

Return codes of the `--quarantine` command:

- -1 – the command is not supported.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

# Actions on quarantined objects

*To perform actions on quarantined objects in Kaspersky Endpoint Agent through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Do the following and press **ENTER**:
   - To permanently delete the quarantined objects, execute the following command:

     `agent.exe --quarantine=delete --ouid=<` comma-separated quarantined object identifiers. Required parameter`> [--pwd=<` current user password`>]`.

     Objects with the specified identifiers will be deleted from the Quarantine folder on the devices. The Quarantine folder is specified when quarantine settings are configured.
   - To restore objects from quarantine, execute the following command:

     `agent.exe --quarantine=restore --ouid=<` comma-separated quarantined object identifiers. Required parameter`> [--path-type=<` one of the destination folder options to restore the objects from the quarantine: `original|custom|settings`. Optional parameter`> --path=<` path to the destination folder for restored objects. Required parameter if the `--path-type` parameter is passed and the `original>] value is specified [--action=<` one of the actions on the object: `replace|rename`. Optional parameter`>] [--pwd=<` current user password`>]`.

- To quarantine an object, execute one of the following commands:

  - `agent.exe --quarantine=add [--file=<` full path to the object you want to quarantine `>] [--pwd=<` current user password `>]`

  - `agent.exe --quarantine=add [--hash=<` hash of the object you want to quarantine. Required parameter. If you do not specify the full path to the object and pass the `--hashalg` parameter `>]--hashalg=<` one of the hash types: `md5|sha256`. Required parameter. If you do not specify the full path to the object `> [--file=<` path to the folder with the object that you want to quarantine `>] [--pwd=<` current user password `>]`.

Command parameters when performing actions on quarantined objects

| Parameter | Description |
|---|---|
| `--ouid` | Required parameter. The parameter passes a unique numeric (int64) identifier of the quarantined object.<br>Displayed when viewing information about quarantined objects (command `--quarantine=show`). |
| `--path-type=<original\|custom\|settings>` | The parameter describes the logic for the destination folder selection when restoring objects from quarantine.<br>• If the parameter is not passed, the object will be restored to the original folder – the folder where the object was located before being quarantined. If the source folder is not available, the object will be restored to the folder specified when configuring quarantine settings.<br>• If the parameter is passed with the `<original>` value, the object will be restored to the original folder – the folder where the object was located before being quarantined. If the source folder is not available, the object will be restored to the folder specified when configuring quarantine settings.<br>• If the parameter is passed with the `<settings>` value, the object will be restored to the folder specified when configuring quarantine settings. If the folder is not available, the task fails.<br>• If the parameter is passed with the `<custom>` value, the object will be restored to the folder, the path to which is specified as the value of the `--path` parameter. If the folder is not available, the task fails. |
| `--path=<` path to the destination folder for restored objects `>` | Required parameter if the `--path-type` parameter is passed with the `<custom>` value.<br>This parameter defines the path where you want to create a folder for objects restored from the quarantine, if you do not want to use the folder where the object was located before being quarantined and the folder specified when configuring quarantine settings. |
| `--action=<replace\|rename>` | This parameter defines the action that you want to perform on the object if the destination folder for restored objects already contains a file with name same to the name of the file you are restoring from quarantine.<br>• If the parameter is not passed, the restored object will be renamed: the `_restored` suffix will be added to the original object name.<br>• If the parameter is passed with the `<rename>` value, the restored object will be renamed: the `_restored` suffix will be added to the original object name.<br>• If the parameter is passed with the `<replace>` value, the original object will be replaced with the restored object. |
| `--file=<` full path to the object you want to quarantine `>` | Required parameter if the `–hashalg` parameter is not passed.<br>The parameter defines the full path to the object that you want to quarantine. |
| `--hashalg=<md5\|sha256>` | Required parameter if the `–file` parameter is not passed and the full path to the object you want to quarantine is not specified.<br>The parameter defines the hashing algorithm to calculate the checksum of the object you want to quarantine.<br>The parameter can be passed with one of the following values: `<md5>` or `<sha256>`. |
| `--hash=<target file checksum>` | Required parameter if the `–hashalg` parameter is passed.<br>The parameter defines the checksum of the object you want to quarantine. |
| `--file=<target file folder>` | Required parameter if the –hashalg parameter is passed.<br>This parameter specifies the path to the folder which contains the object that you want to quarantine and whose hash is specified as the value of the `--hash` parameter. |
| `--pwd=<` current user password `>` | Allows you to specify the password of the user whose account is used to execute the command. |

Return codes of the `--quarantine` command:

- -1 – the command is not supported.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

# Managing Kaspersky Sandbox integration settings

*To manage the integration settings of Kaspersky Endpoint Agent with Kaspersky Sandbox through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   `--sync-period=<sync period>--sandbox=<enable|disable|show> [--tls=<yes|no>] --servers=<address>:<port> [--timeout=<maximum response timeout of Kaspersky Sandbox server>] [--pinned-certificate=<full path to the TLS certificate file for connection between Kaspersky Endpoint Agent and Kaspersky Sandbox>] --pwd=<current user password>`

   Parameters of the `--sandbox` command when managing the integration settings of Kaspersky Endpoint Agent with Kaspersky Sandbox

| Parameter | Description |
|---|---|
| `--sandbox=<enable\|disable\|show>` | Required parameter.<br>Allows you to enable, disable, and view integration status of Kaspersky Endpoint Agent with Kaspersky Sandbox.<br>• `--sandbox=<enable>` – enables integration.<br>• `--sandbox=<disable>` – disables integration.<br>• `--sandbox=<show>` – displays integration status of Kaspersky Endpoint Agent with Kaspersky Sandbox. |
| `---tls=<yes\|no>` | Optional parameter.<br>Allows you to enable or disable trusted connection between Kaspersky Sandbox and Kaspersky Endpoint Agent.<br>• `--tls=<yes>` – enables trusted connection.<br>• `--tls=<no>` – disables trusted connection. |
| `--servers=<address>:<port>` | Required parameter.<br>Allows you to add Kaspersky Sandbox servers to Kaspersky Endpoint Agent list. |
| `--timeout=<maximum response timeout of Kaspersky Sandbox server>` | Optional parameter.<br>Allows you to set the maximum response timeout of Kaspersky Sandbox server in milliseconds. |

| | |
|---|---|
| `--pinned-certificate=<full path to the TLS certificate file for connecting Kaspersky Endpoint Agent with Kaspersky Sandbox>` | Required parameter, if the `--tls` parameter is passed with the `<yes>` value.<br>Allows you to add a TLS certificate for connecting Kaspersky Endpoint Agent with Kaspersky Sandbox. |
| `--pwd=<current user password>` | Allows you to specify the password of the user whose account is used to execute the command. |

# Managing integration settings with KATA Central Node component

*To manage the integration settings of Kaspersky Endpoint Agent with the KATA Central Node component through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Run the following command and press **ENTER**:

   `agent.exe --message-broker=<enable|disable|show> --type=<kata> --compression=<yes|no> --partitioning-strategy=<automatic|user> [--message-key=<message key> --topic=<topic> --partition=<user specific partition>] --tls=<yes|no> --servers=<address>:<port> [--timeout=<maximum response timeout of KATA server ] [--pinned-certificate=<full path to the TLS certificate file>] [--client-certificate=<full path to the certificate file>] --client-password=<password for the PFX archive> --sync-period=<interval for sending synchronization requests>`

   The `--message-broker` command parameters when managing the settings of integration between Kaspersky Endpoint Agent and the KATA Central Node component

| Parameter | Description |
|---|---|
| *`--message-broker=<enable\|disable\|show>`* | Required parameter.<br>Allows you to enable, disable, and view integration status of Kaspersky Endpoint Agent with the KATA Central Node component.<br>• `--message-broker=<enable>` – enables integration.<br>• `--message-broker=<disable>` – disables integration.<br>• `--message-broker=<show>` – displays integration status of Kaspersky Endpoint Agent with the KATA Central Node component. |
| *`--type=<kata>`* | • Required parameter.<br>• Allows you to specify the KATA Central Node component for managing the integration settings of Kaspersky Endpoint Agent with this component. |
| `---tls=<yes\|no>` | Optional parameter.<br>Allows you to enable or disable trusted connection between Kaspersky Endpoint Agent and the KATA Central Node component.<br>• `--tls=<yes>` – enables trusted connection.<br>• `--tls=<no>` – disables trusted connection. |
| `--servers=<address>:<port>` | Required parameter.<br>Allows you to add a KATA server. |
| `--timeout=<maximum response timeout of Kaspersky Anti Targeted Attack Platform server>` | Optional parameter.<br>Allows you to set the maximum response timeout of KATA server in milliseconds. |
| `--pinned-certificate=<full path to the TLS certificate file>` | Required parameter, if the `--tls` parameter is passed with the `<yes>` value.<br>Allows you to add a TLS certificate for connecting Kaspersky Endpoint Agent with KATA server. |

| | |
|---|---|
| `--client-certificate=<` full path to the certificate file > | Allows you to add a user certificate for connecting Kaspersky Endpoint Agent with KATA server. |
| `--pwd=<` current user password > | Allows you to enter the password for the PFX archive, containing a user certificate for connecting Kaspersky Endpoint Agent with KATA server. |
| `--sync-period=<` interval for sending synchronization requests > | Allows you to specify the time interval for sending requests for synchronization Kaspersky Endpoint Agent settings and tasks with KATA Central Node. |

# Running Kaspersky Endpoint Agent database and module update

*To perform Kaspersky Endpoint Agent application database and module update through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Run the following command and press **ENTER**:

   ```
   agent.exe --update=bases|modules [--source=<addresses of custom database update sources separated by semicolons without space>|kl|ksc]
   ```

   Command parameters when running Kaspersky Endpoint Agent database update

| Parameter | Description |
|---|---|
| `--update=bases\|modules` | Required parameter.<br>Allows you to specify the type of update:<br>• `--update=bases` starts application database update.<br>• `--update=modules` starts application module update. |
| `--source=<addresses of custom database update sources>\|kl\|ksc]` | Optional parameter.<br>Allows you to select a database update source.<br>• `--source=<addresses of custom database update sources>` allows you to select the **Custom HTTP or FTP servers or network folders** option as database update source and specify the path to the network folder or IP, FTP or HTTP-address of the server from which the application downloads database updates.<br>You can specify several addresses of custom database update sources separated by a semicolon without a space (";"). The application will download updates from the first available database update source. If all addresses are not available, the task will fail.<br>• `--source=kl` allows you to select the **Kaspersky update servers** option as database update source.<br>If the servers are not available, the task will fail.<br>• `--source=ksc` allows you to select the **Kaspersky Security Center Administration Server** option as database update source.<br>If the Administration Server is not available, the task will fail. |

Return codes of the `--update=bases` command:

- -1 – the command is not supported.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.

- 4 – syntax error.
- 8 – permission error.
- 200 – all objects are valid.
- -206 – update files are not available in the specified database update source or have an unknown format.
- -209 – error connecting to the database update source.
- -232 – error connecting to the proxy server.
- -234 – error connecting to Kaspersky Security Center.
- -236 – application databases are corrupted.

# Starting, stopping and viewing the current application status

*To start, stop, or view the current Kaspersky Endpoint Agent status through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   ```
   agent.exe --product=<start|stop|state> [--pwd=<current user password>]
   ```

   Command parameters when starting, stopping, and viewing the current state of Kaspersky Endpoint Agent

| Parameter | Description |
|---|---|
| `--product=<start\|stop\|state>` | Allows you to start, stop or view the current application status.<br>• `--product=<start>` – starts the application.<br>• `--product=<stop>` – stops the application.<br>If password protection is configured for the application, a password is required to execute the `--product=<stop>` command.<br>• `--product=<state>` – displays the current state of the application: started or stopped. |
| `--pwd=<current user password>` | Allows you to specify the password of the user whose account is used to execute the command. |

Return codes of the `--product=<start|stop|state>` command:

- -1 – the command is not supported.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

- 8 – permission error.
- 9 – invalid operation (for example, an attempt to execute the `--product=start` command, if the application is already running).

# Protecting the application with password

To restrict Kaspersky Endpoint Agent operations, which can result in decrease of protection level of the user computer and the data processed on this computer, as well as decrease of the application self-defense level, it is required to protect the application with password.

Password is required to execute the following commands in Kaspersky Endpoint Agent command line interface:

- `--sandbox=disable`
- `--sandbox=show`
- `--sandbox=enable --tls=no`
- `--sandbox=enable --pinned-certificate=<full path to the TLS certificate file for connecting Kaspersky Endpoint Agent with Kaspersky Sandbox>`
- `--quarantine=delete –ouid`
- `--quarantine=show`
- `--quarantine=restore`
- `--quarantine=add`
- `--product=stop`
- `--password=reset`
- `--isolation=disable`
- `--prevention=disable`
- `--selfdefence`
- `--license=delete`
- `--message-broker --type=kata <settings>`
- `--event --action=enable`
- `--event --action=disable`

To enter the password, use the `--pwd=<current user password>` parameter.

The password is also required when performing the following actions on the application:

- Application uninstallation and remote application uninstallation using Kaspersky Security Center
- Changing the set of the application components (`modify`)
- Application update (`upgrade`)
- Application repair (`repair`)
- Operations in the application installation wizard
- Operations in the command line interface

After enabling password protection and applying Kaspersky Security Center policy, a single password is applied to all devices of Kaspersky Endpoint Agent managed group.

Changing password protection settings (disabling password protection or changing the password) is not available on local devices.

After disabling password protection in the policy, password protection settings retain for the local device and can be edited.

The password is stored in the application settings in encrypted form (as a checksum).

To enter the password, use the `--pwd=<current user password>` parameter.

*To configure Kaspersky Endpoint Agent password protection through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Enter one of the following commands and press **ENTER**:
   - `agent.exe --password=stat` to view the current password protection status of the application.
   - `agent.exe --password=set --pwd=<current user password> --new=<new user password>` to set a new user password.
   - `agent.exe --password=reset --pwd=<current user password>` to reset the user password.

# Protecting application services with PPL technology

Protection of services (for example, the soyuz.exe service) using the *Protected Process Light (PPL)* technology is implemented in Kaspersky Endpoint Agent.

Processes that are running with the PPL flag cannot be stopped or changed by other processes without the PPL flag.

Usage of the PPL flag for the application services allows you to protect the services from malicious external influences and attempts to compromise the application.

*To configure protection of application services by the PPL technology through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Enter one of the following commands and press **ENTER**:

   - `agent.exe --ppl=show [--pwd=<current user password>]`, to view the current status of application services protection by the PPL technology.

   - `agent.exe --ppl=disable [--pwd=<current user password>]`, to disable the application services protection by the PPL technology.

Return codes of the `--ppl` command:

- 0 – command successfully executed.
- 2 – general error.
- 4 – syntax error.
- 8 – permission error.

# Managing self-defense settings

*To manage self-defense settings through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Run the following command and press **ENTER**:

   `agent.exe --selfdefence=<enable|disable>`

# Managing event filtering

*To manage event filtering through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   ```
   agent.exe --event =
   <createprocess|loadimage|registry|network|eventlog|filechange|accountloggon|codeinjecti
   --action=<enable|disable|show>
   ```

# Managing network isolation

*To obtain information on the current network isolation state through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.
2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Type the following command: `agent.exe --isolation=show` and press **ENTER.**

   Displays the current network isolation settings of the device in the console, including the list of the specified exclusion network profiles, as well as the list of rules defined in the network profiles.

Return codes of the `--isolation` command:

- -1 – the command is not supported by Kaspersky Endpoint Agent version installed on the device.
- 0 – command successfully executed.
- 1 – a required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.
- 9 – invalid operation (for example, an attempt to disable network isolation if network isolation is not enabled).

# Managing Standard IOC Scan tasks

*Standard IOC Scan tasks* are created manually in Kaspersky Security Center or through the command line interface.

*To create and configure a Standard IOC Scan task through the command line interface:*

1. On the device, run a command line interpreter (for example, Command Prompt cmd.exe) with the permissions of the local administrator.

2. Using the `cd` command, navigate to the folder where the Agent.exe file is located.

   For example, you can type the following command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Run the following command and press **ENTER**:

   ```
   agent.exe --scan-ioc {[--path=<path to the folder with IOC files>] | [<full path to the IOC file>]} [--process=no] [--hint=<full path to the process executable file|full path to the file>] [--registry=no] [--dnsentry=no] [--arpentry=no] [--ports=no] [--services=no] [--system=no] [--users=no] [--volumes=no] [--eventlog=no] [--datetime=<event publication date>] [--channels=<list of channels>] [--files=no] [--drives=<all|system|critical|custom>] [--excludes=<list of exclusions>][--scope=<configurable list of folders>]
   ```

   If the `--scan-ioc` command is passed only with the required parameters, Kaspersky Endpoint Agent performs scanning with the default settings.

   If the `--scan-ioc` command is passed with the two required parameters at the same time (`--path=<path to the folder with IOC files>` and `<full path to the IOC file>`), Kaspersky Endpoint Agent scans all the submitted IOC files.

   Command parameters for running and configuring Standard IOC Scan tasks

| Parameters | Description |
|---|---|
| `--scan-ioc` | Required parameter.<br><br>Starts the Standard IOC Scan tasks on the device. |
| `--path=<path to the folder with IOC files>` | Path to the folder with the IOC files that you want to scan.<br><br>Required parameter, if the `<full path to the IOC file>` parameter is not specified. |
| `<full path to the IOC file>` | Full path to the IOC file with the ioc or xml extension that you want to scan.<br><br>Required parameter, if the `--path=<path to the folder with IOC files>` parameter is not specified.<br><br>Passed without the `--path` argument. |
| `--process=<no>` | Optional parameter.<br><br>The parameter disables the analysis of process data during scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not consider the processes running on the device when scanning. If the IOC file contains IOC terms of the ProcessItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans the process data only if the ProcessItem IOC document is described in the IOC file submitted for scan. |

| | |
|---|---|
| `--hint=<full path to the process executable file\|full path to the file>` | Optional parameter.<br><br>The parameter allows you to narrow the scope of analyzed data for checking the ProcessItem and FileItem IOC documents, by specifying a particular file.<br><br>The parameter value can be set as:<br><br>• `<full path to the executable process file>` – ProcessItem<br>• `<full path to the file>` – FileItem<br>The parameter can only be passed together with the `--process=yes` and `--files=yes` arguments. |
| `--dnsentry=no` | Optional parameter.<br><br>The parameter disables analysis of data on records in local DNS cache (DnsEntryItem IOC document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not scan local DNS cache. If the IOC file contains the terms of the DnsEntryItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans local DNS cache only if the DnsEntryItem IOC document is described in the IOC file submitted for scan. |
| `--arpentry=no` | Optional parameter.<br><br>The parameter disables analysis of data on records in the ARP table (ArpEntryItem document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not scan the ARP table. If the IOC file contains the terms of the ArpEntryItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans the ARP table only if the ArpEntryItem IOC document is described in the IOC file submitted for scan. |
| `--ports=no` | Optional parameter.<br><br>The parameter disables analysis of data on ports that are open for listening (PortItem document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not scan the table of active connections on the device. If the IOC file contains the terms of the PortItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans the table of active connections only if the PortItem IOC document is described in the IOC file submitted for scan. |
| `--services=no` | Optional parameter.<br><br>The parameter disables analysis of data on services installed on the device (ServiceItem document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not scan data on services installed on the device. If the IOC file contains the terms of the ServiceItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans the data on services only if the ServiceItem IOC document is described in the IOC file submitted for scan. |
| `--volumes=no` | Optional parameter.<br><br>The parameter disables analysis of volume data (VolumeItem document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not scan volume data on the device. If the IOC file contains the terms of the VolumeItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans the data on volumes only if the VolumeItem IOC document is described in the IOC file submitted for scan. |

| | |
|---|---|
| `--eventlog=no` | Optional parameter.<br><br>The parameter disables analysis of data about Windows Event Log entries (EventLogItem document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not scan Windows Event Log entries. If the IOC file contains the terms of the EventLogItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans Windows Event Log entries only if the EventLogItem IOC document is described in the IOC file submitted for scan. |
| `--datetime=<event publication date>` | Optional parameter.<br><br>The parameter allows you to enable or disable accounting for date and time when the event was registered in the Windows Event Log when determining the IOC scan area for the corresponding IOC document.<br><br>During IOC scan, Kaspersky Endpoint Agent will only process the events that were registered within the time interval between the specified date and time and the task execution time.<br><br>Kaspersky Endpoint Agent allows you to specify the event registration date as the parameter value. Scan will be performed only for the events registered in the Windows Event Log between the specified date and the time when IOC scan is performed.<br><br>If the parameter is not passed, Kaspersky Endpoint Agent scans events with any registration date. The TaskSettings::BaseSettings::EventLogItem::datetime parameter cannot be changed.<br><br>This parameter is used only if the EventLogItem IOC document is described in the IOC file submitted for scan. |
| `--channel=<list of channels>` | Optional parameter.<br><br>This parameter allows you to pass a list of the names of channels (logs) for which IOC scan is required.<br><br>If this parameter is passed, Kaspersky Endpoint Agent considers only the events published in the specified logs when performing the IOC Scan task.<br><br>The name of the log is specified as a string, in accordance with the name of the log (channel) specified in the properties of this log (the Full Name parameter) or in the properties of the event (the <Channel></Channel> parameter in the xml-scheme of the event).<br><br>By default (including the case if the parameter is not passed), IOC scan is performed for the Application, System, and Security channels.<br><br>Several values separated by space can be passed to the parameter.<br><br>This parameter is used only if the EventLogItem IOC document is described in the IOC submitted for scan. |
| `--system=no` | Optional parameter.<br><br>The parameter disables analysis of environment data (SystemInfoItem IOC document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not analyze environment data. If the IOC file contains the terms of the SystemInfoItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent analyzes environment data only if the SystemInfoItem IOC document is described in the IOC file submitted for scan. |

| | |
|---|---|
| `--users=no` | Optional parameter.<br><br>The parameter disables analysis of user data (UserItem IOC document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not analyze data on the users created in the system. If the IOC file contains the terms of the UserItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent analyzes data on the users created in the system only if the UserItem IOC document is described in the IOC file submitted for scan. |
| `--files=no` | Optional parameter.<br><br>The parameter disables analysis of data on files (FileItem IOC document) during IOC scan.<br><br>If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not analyze data on files. If the IOC file contains the terms of the FileItem IOC document, they are ignored (defined as no match).<br><br>If the parameter is not passed, Kaspersky Endpoint Agent analyzes data on files only if the FileItem IOC document is described in the IOC file submitted for scan. |
| `--drives=<all\|system\|critical\|custom>` | Optional parameter.<br><br>The parameter allows you to specify the IOC scan scope when analyzing data for the FileItem IOC document.<br><br>The parameter can have one of the following values:<br><br>• `<all>` – the application scans all available file areas.<br>• `<system>` – the application scans only the files that are located in the folders where the operating system is installed.<br>• `<critical>` – the application scans only temporary files that are located in user and system folders.<br>• `<custom>` – the application scans only the files that are located in the areas specified by the user.<br>If the parameter is not passed, critical areas are scanned. |
| `--Excludes=<list of exclusions>` | Optional parameter.<br><br>The parameter allows you to specify exclusion scopes when analyzing data for the FileItem IOC document. Several values separated by space can be passed by the parameter.<br><br>If the parameter is not passed, all folders are scanned, with no exclusions. |
| `--scope=<configurable list of folders>` | Optional parameter.<br><br>The parameter becomes required if the `--drives=custom` parameter is passed.<br><br>The parameter allows you to specify a list of scan areas. Several values separated by space can be passed by the parameter. |

Return codes of the `--scan-ioc` command:

- `-1` – the command is not supported by Kaspersky Endpoint Agent version installed on the device.
- `0` – command successfully executed.
- `1` – a required argument is not passed to the command.
- `2` – general error.
- `4` – syntax error.

If the command execution completed successfully (code `0`) and indicators of compromise were detected during to command execution, Kaspersky Endpoint Agent displays the following data on the task execution results in the command line:

Data displayed by the application in the command line when IOC is detected.

| | |
|---|---|
| `Uuid` | IOC file identifier from the header of the IOC file structure (`<ioc id="">` tag) |
| `Name` | IOC file description from the header of the IOC file structure (`<description></description>` tag) |
| `Matched Indicator Items` | The list of identifiers of all triggered indicators. |
| `Matched objects` | Data on each IOC document for which a match was found. |

# 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:

- The program database.
- Objects in Storage.
- Files from alerts generated during a rescan.
- Sandbox artifacts.
- Configuration files.
- Information about KATA and KEDR licenses.
- 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:

- The program database.
- Objects in Storage.
- Files from alerts generated during a rescan.
- Sandbox artifacts.
- Configuration files.
- Information about KATA and KEDR licenses.
- Central Node or PCN settings.

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<br><br>The program database on Central Node:<br><br>• Alerts and VIP statuses of alerts<br>• Task execution results<br>• Policies<br>• User-defined TAA (IOA) rules and exclusions<br>• User-defined IDS rules and exclusions<br>• IOC files<br>• Object white lists<br>• Information about files in Storage<br>• Information about quarantined objects<br>• List of computers with Endpoint Agent<br>• Reports and report templates<br>• Notifications | Central Node settings, if selected.<br>Program databases, by default. | Standalone Central Node server. |
| 4 GB | PCN settings. | Custom | Distributed solution and multitenancy mode. |
| 4 GB | SCN settings. | Custom<br>As for a standalone Central Node server. | Distributed solution and multitenancy mode. |
| 4 GB | Program databases on the PCN:<br><br>• Alerts and VIP statuses of alerts<br>• Task execution results<br>• Policies<br>• User-defined TAA (IOA) rules and exclusions<br>• User-defined IDS rules and exclusions<br>• IOC files<br>• Object white lists<br>• Information about files in Storage<br>• Information about quarantined objects<br>• List of computers with Endpoint Agent<br>• Reports and report templates<br>• Notifications | Default | Distributed solution and multitenancy mode. |
| No | Configuration files. | Yes | All modes. |

| Maximum data volume | Data type | Exported data | Program operation mode |
|---|---|---|---|
| No | KATA and KEDR licenses. | Yes | All modes. |
| 300 GB | Backup | Custom | All modes. |
| 300 GB | Sandbox artifacts. | Custom | All modes. |
| 300 GB | Files from alerts generated during a rescan. | Custom | All modes. |
| No | 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:*

1. In the list of sections of the program administrator menu, select the **System administration** section.
2. Press **ENTER**.
   This opens the action selection window.
3. In the list of actions, select **Backup/Restore settings**.
4. Press **ENTER**.
   This opens the **Backup/Restore settings** window.
5. In the list of actions, select **New**.
6. Press **ENTER**.
   This opens the **Backup settings** window.
7. Click **Back up**.

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, 2020 at 10 hours 00 minutes 00 seconds:

```
scp admin@10.0.0.10:settings-20200410-100000.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, 2020 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-20200410-100000.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 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 of the server:*

1. In the list of sections of the program administrator menu, select the **System administration** section.
2. Press **ENTER**.

   This opens the action selection window.
3. In the list of actions, select **Backup/Restore settings**.
4. Press **ENTER**.

   This opens the **Backup/Restore settings** window.
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**.

   This opens the action selection window.
7. In the list of actions, select **Restore <name of the file with the backup copy of the program>**.
8. Press **ENTER**.

   This opens the action confirmation window.
9. Click **Restore**.

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 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.

Parameters of the command for creating a backup copy of Kaspersky Anti Targeted Attack Platform

| Required parameter | Parameter | Description |
|---|---|---|
| Yes | `-b <path>` | Create a file containing a backup copy of the program at the specified path,<br>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. |
| No | `-q` | Save files in quarantine. |

| | | |
|---|---|---|
| No | `-a` | Save files awaiting rescan. |
| No | `-s` | Save Sandbox artifacts. |
| No | `-n` | Save Central Node or PCN settings. |
| No | `-l <filepath>` | 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_ddmmyyyyhhMM, 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 KATA3.7.sql for the backup copy of the program version 3.7.

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 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.

Parameters of the command for restoring Kaspersky Anti Targeted Attack Platform from a backup copy

| Required parameter | Parameter | Command description |
|---|---|---|
| Yes | `-r <path>` | Restore data from a file containing a backup copy of the program,<br>where <path> is the absolute path or relative path to the folder containing the file |
| No | `-c <path>` | Prior to starting restoration of the program, clear the folder at the specified path,<br>where <path> is the absolute path or relative path to the folder in which the program upgrade file is created.<br>After this command is executed, the program also checks for free disk space. |
| No | `-l <filepath>` | 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. |

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 3.7 to version 3.7.1. Upgrading the program involves the following steps:

1. Updating the Sandbox component

   The program does not have a standard upgrade procedure. You must install the component version 3.7.1.

   > After installing the component you need to set the maximum number of simultaneously running virtual machines. The value 48 is used by default.

   > When installing the component on a VMware ESXi virtual machine, you must set up a configuration described in *Calculations for the Sandbox component* section.

2. Upgrading the Central Node component

   > You can upgrade the component to version 3.7.1 only from version 3.7. If you are using an older version, you must upgrade it to 3.7.1: 3.6 → 3.7 and 3.7 → 3.7.1.

   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:

   a. 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.

   b. 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.

   c. 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.

      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. To do so, in the web interface of the PCN server:

      a. Add the relevant organizations.

      b. Configure the access of user accounts with the **Senior security officer** and **Security officer** roles to these companies and servers.

c. Delete all SCNs that are temporarily disconnected from the PCN during the update.

d. Re-connect all relevant SCNs to the PCN.

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.

3. Upgrading the Sensor component installed on a standalone server

   The program does not have a standard upgrade procedure. You must install the component version 3.7.1 from scratch.

4. Upgrading Kaspersky Endpoint Agent for Windows

# Installing program update packages in the administrator menu and in Technical Support Mode

When Kaspersky 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 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**.

   This opens the Technical Support Mode confirmation window.

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 `scp apt-system-3.7.0-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, and to provide access to information about all alerts 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.

# 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:

1. **Authorization of the external system**

   The administrator must create a request to integrate the external system with the program. Then the program administrator must process the request in the web interface of Kaspersky Anti Targeted Attack Platform.

2. **Creating a request for scanning objects using the `HTTP POST` method**

3. **Creating a request for scan results using the HTTP `GET` method**

   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 HTTP `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 about detected objects in the web interface of Kaspersky Anti Targeted Attack Platform.

4. **Creating a request to delete scan results using the HTTP `DELETE` method**

   You can delete the results of scanning a specified object or all objects.

# Integrating an external system with Kaspersky Anti Targeted Attack Platform

To start working with the API, you need to integrate an external system with Kaspersky Anti Targeted Attack Platform. The external system must complete authorization on the Kaspersky Anti Targeted Attack Platform server.

*To integrate the 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.
3. Create any request containing a `sensorId` from the external system in Kaspersky Anti Targeted Attack Platform. For example, you can create a request to scan an object from an external system in Kaspersky Anti Targeted Attack Platform.

   The web interface of Kaspersky Anti Targeted Attack Platform will display the request for authorization from the external system. Contact the program administrator to process the request.

If you need to change the external system server certificate, repeat the steps for integrating the external system with Kaspersky Anti Targeted Attack Platform.

# 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 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. Return code 413 is generated when the HTTP `POST` method is created. You can find out the maximum allowed size of an object by using the `GET` method to view the list of object scan restrictions.

# Request to scan objects

To create a request for scanning objects, the HTTP `POST` method is used. You can create a request by using the cURL command-line utility, for example.

You can set the parameters for executing a cURL command by using additional switches (see the table below).

Please refer to the cURL documentation for more information about cURL command switches.

## Command syntax

```
curl --cert <path to the TLS certificate file> --key <path to the private key file> -X
POST "<URL of the server with the Central Node component>:<default port
443>/kata/scanner/v1/sensors/<sensorId>/scans?sensorInstanceId=<sensorInstanceId>" -F
"content=<path to the file that you want to scan>" -F scanID=<scan request ID> -F
"objectType=file"
```

If the request is processed successfully, the `OK` status will be displayed.

## Parameters

| Parameter | Type | Description |
|---|---|---|
| `sensorId` | string | Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform. |
| `content` | file | Contents of the scanned object. |
| `scanId` | string | Unique ID of the scan request. It must be generated in the external system. It cannot contain spaces or special characters. Do not use file names as a scan request ID.<br>If this parameter is not defined, viewing scan results is not available. |
| `objectType` | string | Type of scanned object.<br>Possible value of the parameter: `file`. |
| `sensorInstanceId` | 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. |

## 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. |

### Example of entering a command with switches

```
curl --cert /root/cert.pem --key /root/server.key -
X POST "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?
sensorInstanceId=instance1" -F "content=@/tmp/test" -F scanId=1 -F "objectType=file"
```

## Request for scan results

To create a request for receiving scan results, the HTTP `GET` method is used. You can create a request by using the cURL command-line utility, for example.

You can set the parameters for executing a cURL command by using additional switches (see the table below).

Please refer to the cURL documentation for more information about cURL command switches.

### Command syntax

```
curl --cert <path to the TLS certificate file> --key <path to the private key file> -X
GET<URL of the server with the Central Node component>:<default port
443>/kata/scanner/v1/sensors/<sensorId>/scans/state?sensorInstanceId=
<sensorInstanceId>&state=<one or more scan statuses that you want to display in scan
results>"
```

If the request is sent successfully, a list of requests for scanning objects and the results of scanning these objects will be displayed. The scan results will be filtered by the statuses that you specified in the `state` parameter. For example, if you specified `state = processing, detect` in the request for scan results, the program will display only the object scan requests that are being processed or in which the program has detected a threat.

### Parameters

| Parameter | Type | Description |
|---|---|---|
| `sensorId` | string | Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform. |
| `state` | array (string element type) | Object scan status. When this parameter is defined, the scan results will be filtered by status.<br>Indicate one or more statuses separated by commas.<br>The following parameter values are available:<br>• `detect`;<br>• `not detected`;<br>• `processing`;<br>• `timeout`;<br>• `error`. |
| `sensorInstanceId` | 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. |

### 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. |

### Example of entering a command with switches if you want to display all object scan statuses in the scan results

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans?sensorInstanceId=instance1?&state=detect,not detected,processing,error,timeout"
```

## Request to delete scan results

To create a request to delete the scan results for one or more objects, use the `DELETE` method. You can create a request by using the cURL command-line utility, for example.

### Command syntax

```
curl --cert <path to the TLS certificate file> --key <path to the private key file> -X DELETE "<URL of the server with the Central Node component>:<default port 443>/kata/scanner/v1/sensors/<sensorId>/scans/<scanId>"
```

If the request is processed successfully, the object scan results will be deleted. The `OK` status is displayed.

### 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 object scan request. 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. |

### Command input example

```
curl --cert /root/cert.pem --key /root/server.key -
X DELETE "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/1"
```

## Request to display object scan restrictions

To create a request to display the program's restrictions on scanning objects (for example, by size), the HTTP `GET` method is used. You can create a request by using the cURL command-line utility, for example.

### Command syntax

```
curl --cert <path to the TLS certificate file> --key <path to the private key file> -X
GET "<URL of the server with the Central Node component>:<default port
443>/kata/scanner/v1/sensors/<sensorId>/scans/filters"
```

If the request is processed successfully, the program's object scan restrictions will be displayed. For example, the `maxObjectSize` restriction is the maximum allowed size of an object that you can submit for scanning.

### 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. |

### Command input example

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/scans/filters"
```

# 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.

# Request to display alert information

To create a request to display information about Kaspersky Anti Targeted Attack Platform alerts, the HTTP `GET` method is used. You can create a request by using the cURL command-line utility, for example.

## Command syntax

```
curl --cert <path to the TLS certificate file> --key <path to the private key file> -X GET "<URL of the server with the Central Node component>:<default port 443>/kata/scanner/v1/sensors/<sensorId>/detects?detect_type=<one or more technologies that were used to generate the alert>&limit=<number of alerts in the response to the request>&token=<request ID>"
```

If the request is processed successfully, you will see a list of alerts generated by Kaspersky Anti Targeted Attack Platform on the server of the external system.

## Parameters

| Parameter | Type | Description |
|---|---|---|
| `sensorId` | String | Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform. |
| `detect_type` | Array | Technology that was used to generate the alert. You can specify a comma-separated list of technologies.<br>Possible values:<br>• `am` – Anti-Malware Engine<br>• `sb` – Sandbox<br>• `yara` – YARA<br>• `url_reputation` – URL Reputation<br>• `ids` – Intrusion Detection System<br>If the parameter is not specified, information about all alerts is provided. |
| `limit` | Integer | Number of objects for which information is provided in response to the request. Allowed values: integers from 1 to 10000.<br>The default value is `1000`. |
| `token` | 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.<br>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. |

### Example of entering a command with switches

```
curl --cert /root/cert.pem --key /root/server.key -X GET "https://10.10.10.1:443/kata/scanner/v1/sensors/dd11a1ee-a00b-111c-b11a-11001b1f1111/detects?detect_type=am,sb&limit=100&token=7b226f6666736574223a20307d"
```

# Scope of transmitted data

Information that is transmitted for each alert is listed in the following table.

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:<br>• `high`<br>• `medium`<br>• `low` | Alert importance. |
| `objectSource` | One of the following values:<br>• `web`<br>• `mail`<br>• `endpoint`<br>• `external`<br>• `dns` | Source of the detected object. |
| `technology` | One of the following values:<br>• `am` – Anti-Malware Engine<br>• `sb` – Sandbox<br>• `yara` – YARA<br>• `url_reputation` – URL Reputation<br>• `ids` – Intrusion Detection System<br>• `taa` – Targeted Attack Analyzer | Technology that was used to detect the object. |
| `objectType` | One of the following values:<br>• `file`.<br>• `URL`.<br>• `host` (for remote domains or hosts). | Type of detected object |
| `object` | Depends on the type of detected object. | Data on the detected object. |
| `detection` | Depends on the technology that was used to detect the object. | Data on detected threats. |
| `details` | Depends on the source of detected object. | Data on the environment of detected objects. |

## 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.

| | 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 | SHA256 | SHA256 hash of the file or composite object that was sent for scanning. | 7bbfc1d690079b0c591e146c4294305da1cee857e12db401 |
| | 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 |
| | detectedObject.fileName | String | Name of the file (simple object or file within a composite object) in which the threat was detected. | EICAR-CURE.com |
| | detectedObject.fileSize | Integer | Size of the file (simple object or file within a composite object) in which the threat was detected, in bytes. | 184 |
| URL | detectedObject | String | URL of the detected object. | http://example.com/link |
| host | detectedObject | Array | List of domains to which detected objects belong.<br>• For the TAA technology, only one domain is listed.<br>• For the URL technology, as well as for objects with the objectSource=dns parameter, the list can contain several domains. | example.org, example.net |

# 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.

| Technology | Parameter | Description | Data type | Example |
|---|---|---|---|---|
| One of the following technologies:<br>• Anti-Malware Engine.<br>• YARA.<br>• 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.

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 |
| | URL | URL of the web resource that was accessed.<br>IDS technology alerts do not have this parameter.<br>For URL technology alerts, this parameter has the same value as the detectedObject parameter. | String | https://example.com:443/ |
| | method | HTTP request method. | String | Connect |
| | referrer | URL from which the redirect was made. | String | https://example.com:443/ |
| | agentString | User agent header of the HTTP request that contains the name and version of the client application. | String | Mozilla/4.0 |
| mail | mailFrom | Sender's email address. | String | sender@example.com |
| | mailTo | Comma-separated list of recipient email addresses. | Array | recipient1@example.com, recipient2@example.com |
| | subject | Subject of the message. | String | 'You are the winner' |
| | messageId | Email message ID. | String | 1745028736.156014.1542897410859.JavaMail.svc_jira_poo |
| • endpoint<br>• 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 |

| Source of the object | Parameter | Description | Data type | Example |
| --- | --- | --- | --- | --- |
| 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:<br>• Request<br>• Response | String | Request |
| | dnsRequestType | One of the following DNS request types:<br>• A.<br>• AAA.<br>• CNAME.<br>• MX. | String | MX |
| | domainToBeResolved | Domain name from the DNS request. | String | example.com |

# Sources of information about the program

## Kaspersky Anti Targeted Attack Platform page on the Kaspersky website

On the Kaspersky Anti Targeted Attack Platform page, you can find general information about the program, its capabilities and features.

The Kaspersky Anti Targeted Attack Platform page contains a link to the online store. There you can purchase or renew the program.

## Kaspersky Anti Targeted Attack Platform page in the Knowledge Base

*Knowledge Base* is a section on the Technical Support website.

On the Kaspersky Anti Targeted Attack Platform page in the Knowledge Base, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the program.

Knowledge Base articles can answer questions related not only to Kaspersky Anti Targeted Attack Platform but also to other Kaspersky applications. Knowledge Base articles may also contain news from Technical Support.

## Discussion of Kaspersky software in the user community

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users in our community.

In the community, you can view existing topics, post comments, and create new discussion topics.

# 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 Kaspersky Anti Targeted Attack Platform, we recommend that you contact Technical Support. Technical Support staff will answer your questions about installing and using Kaspersky Anti Targeted Attack Platform.

Kaspersky provides support of Kaspersky Anti Targeted Attack Platform throughout its life cycle (see the program life cycle page). Before contacting Technical Support, please read the support rules.

You can contact Technical Support in one of the following ways:

- visit Technical Support website;
- By sending a request to Technical Support through the Kaspersky CompanyAccount portal.

## Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky experts through online requests. The Kaspersky CompanyAccount portal allows monitoring the progress of online request processing by Kaspersky staff and keeping the 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 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.

# Glossary

## 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.

## Backdoor program

A program planted by hackers on a compromised computer in order to be able to access this computer in the future.

## 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.

## 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.

## End User License Agreement

Binding agreement between you and AO Kaspersky Lab, stipulating the terms on which you may use the program.

## 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.

## IOC

Indicator of Compromise. A set of data about a malicious object or malicious activity.

## IOC file

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.

## 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 Endpoint Agent

Program component. Installed on workstations and servers of the corporate IT infrastructure that run the Microsoft Windows operating system. Continuously monitors processes running on those computers, active network connections, and files that are modified.

## Kaspersky Private Security Network

A solution that allows users of Kaspersky 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 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 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 applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

## Kaspersky Threat Intelligence Portal

Kaspersky information system Contains and displays reputation information for files and URL addresses.

## KATA

Kaspersky Anti Targeted Attack. Functional block of the Kaspersky Anti Targeted Attack Platform program, which detects threats on the perimeter of 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.

## 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.

## 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 (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.

## 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.

## OpenIOC

An open, XML-based standard for describing indicators of compromise containing over 500 different indicators of compromise.

## 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.

## 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.

## TAA (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. A TAA (IOA) rule contains a description of a sign of an attack and recommended countermeasures.

## 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. Analyzes and monitors network activity of software installed on computers of the corporate LAN using TAA (IOA) rules. 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.

## 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.

## 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.

## 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.

# 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.

Apple, Mac, Macintosh, and Safari are trademarks of Apple Inc. registered in the United States and elsewhere.

Snort is a trademark of Cisco Systems, Inc. and/or its affiliates, registered in the USA and elsewhere.

Citrix, Citrix Hypervisor, 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.

Google and Google Chrome are trademarks of Google, Inc.

Intel, Xeon 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.

McAfee is the trademark or registered trademark of McAfee, Inc. in the USA and elsewhere.

Microsoft, Active Directory, Excel, Hyper-V, PowerPoint, PowerShell, Win32, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries.

Mozilla and Firefox are trademarks of the Mozilla Foundation.

Oracle is a registered trademark of the Oracle Corporation and/or its affiliates.

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.

Debian is a registered trademark of Software in the Public Interest, Inc.

SUSE is a trademark of SUSE LLC registered in the United States and elsewhere.

Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

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.