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
- Using Kaspersky Threat Intelligence Portal
- Distribution kit
- Hardware and software requirements
  - Requirements for Kaspersky Endpoint Agent for Windows
  - Compatibility of Kaspersky Endpoint Agent for Windows versions with Kaspersky Anti Targeted Attack Platform versions
  - Compatibility of Kaspersky Endpoint Agent for Windows versions with EPP applications
  - Compatibility of Kaspersky Endpoint Agent for Windows versions with other applications
  - Requirements for Kaspersky Endpoint Agent for Linux
  - Compatibility of Kaspersky Endpoint Agent for Linux versions with Kaspersky Anti Targeted Attack Platform versions
  - Compatibility of Kaspersky Endpoint Agent for Linux versions with EPP applications
  - Compatibility of Kaspersky Endpoint Agent for Linux versions with other applications
  - Compatibility of Kaspersky Endpoint Security for Windows versions with Kaspersky Anti Targeted Attack Platform versions
- Limitations of the current version of the application

Data provision

- Service data of the application
- 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
- Sandbox component data
- Data transmitted between program components
- Data contained in application trace files
- Data of Kaspersky Endpoint Agent for Windows
  - Data received from the Central Node component
  - Data in fields of Windows Event Log events of Kaspersky Endpoint Agent
  - Data in Kaspersky Endpoint Agent for Windows requests to Kaspersky Anti Targeted Attack Platform
  - Service data of Kaspersky Endpoint Agent for Windows
  - Data contained in Kaspersky Endpoint Agent for Windows trace files and dumps
  - Data sent to Kaspersky if the KSN Statement was accepted
  - Data in alerts and events
  - Data contained in task completion reports
  - Data on files that are blocked from starting
  - Data related to the performance of tasks
- Data of Kaspersky Endpoint Agent for Linux
  - Data in Kaspersky Endpoint Agent for Linux requests to Kaspersky Anti Targeted Attack Platform
  - Service data of Kaspersky Endpoint Agent for Linux
  - Data contained in Kaspersky Endpoint Agent for Linux trace files and dumps

Application 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
Architecture of the application
Sensor component
Central Node component
Sandbox component
Kaspersky Endpoint Agent component
Operation of the program
Distributed solution and multitenancy
Distributed solution and multitenancy mode transition scenario
Modifications of program settings for the distributed solution and multitenancy mode
Assigning the PCN role to a server
Assigning the SCN role to a server
Processing SCN to PCN connection requests
Viewing information about tenants, PCN and SCN servers
Adding a tenant to the PCN server
Deleting a tenant from the PCN server
Renaming a tenant 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 application
Preparing for installing application 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
Installing the 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 controlling 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
Deploying the Central Node component with Embedded Sensor as a cluster
Deploying a storage server
Step 2. Selecting a server role
Step 3. Selecting the deployment mode
Step 4. Selecting a disk for installing the component
Step 1. Viewing the End User License Agreement and Privacy Policy
Step 5. Selecting a network mask for server addressing
Step 6. Selecting a network mask for addressing of application components
Step 7. Selecting the cluster network interface
Step 8. Selecting the external network interface
Step 9. Selecting the method of obtaining IP addresses for network interfaces
Step 10. Creating an administrator account and authenticating the server in the cluster
Creating the administrator account
Authenticating the server in the cluster
Step 11. Adding DNS server addresses
Step 13. Selecting disks for the Ceph storage
Deploying the processing server
Step 2. Selecting a server role
Step 2. Selecting the deployment mode
Step 3. Selecting a disk for installing the component
Step 1. Viewing the End User License Agreement and Privacy Policy
Step 5. Selecting a network mask for server addressing
Step 6. Selecting a network mask for directing program components
Step 7. Selecting the cluster network interface
Step 8. Selecting the external network interface
Step 9. Selecting the method of obtaining IP addresses for network interfaces
Step 9. Authenticating the server in the cluster
Configuring receipt of mirrored traffic from SPAN ports
Step 12. Adding DNS server addresses

Installing the Central Node component with Embedded Sensor on a server
Step 2. Selecting a server role
Step 1. Viewing the End User License Agreement and Privacy Policy
Step 3. Selecting a disk for installing the component
Step 4. Allocating the disk for the Targeted Attack Analyzer component's database
Step 5. Selecting a network mask for cluster server addressing
Step 7. Selecting the external network interface
Step 8. Selecting the method of obtaining IP addresses for network interfaces
Step 9. Creating the administrator account
Step 11. Adding DNS server addresses
Step 10. Configuring receipt of mirrored traffic from SPAN ports
Step 12. Configuring time synchronization with an NTP server
Installing the Sensor component on a standalone server
Step 2. Selecting a server role
Step 1. Viewing the End User License Agreement and Privacy Policy
Step 3. Selecting a disk for installing the component
Step 6. Selecting the external network interface
Step 5. Connecting to the server with the Central Node component
Step 6. Creating the administrator account
Configuring the sizing settings of the program
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 the Endpoint Agent component to the Sensor server
Enabling 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 your own TLS certificate 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 application
Getting started with the web interface for sizing management
Getting started with the application web interface with a local administrator account
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
Configuring user account table display
Viewing the user account table
Filtering user accounts
Clearing the account filter
Changing access rights of a program web interface user account
Enabling or disabling a user account
Changing the password of a program administrator or user account
Changing the password of your account
Authentication using domain accounts
Creating a keytab file
Configuring integration with Active Directory
Disabling integration with Active Directory
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
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 the administrator: Getting started in the program web interface
Kaspersky Anti Targeted Attack Platform Interface
Monitoring program operation
About widgets and layouts
Selecting a tenant 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 data display period 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
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
Configuring the mail server connection
Selecting operating systems to use when scanning objects in Sandbox
Managing the Sensor component
Viewing the table of servers with the Sensor component
Processing a connection request from 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 the cluster
Viewing the table of servers of the cluster
Adding a server to a cluster
Increasing the disk space on the storage server
Decommissioning servers
Removing a server from a cluster
Starting up and shutting down the cluster
Notifications about the maximum allowed CPU and RAM load for the Central Node and Sensor servers
Configuring the maximum allowable CPU and RAM load of the Central Node and Sensor servers
Configuring the SNMP protocol connection
Description of MIB objects of Kaspersky Anti Targeted Attack Platform
Managing Kaspersky Endpoint Agent host information
Selecting a tenant 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 information logging to a remote log
Configuring the main settings for SIEM system integration

- Uploading a TLS certificate
- Enabling and disabling TLS encryption of the connection with the SIEM system
- Content and properties of syslog messages about alerts
- Managing the application user activity log
- Enabling and disabling the recording of information in the activity log
- Downloading the activity log file
- Content and properties of CEF messages about user activity in the web interface
- Database Update
- Selecting a database update source
- Updating databases manually
- Creating a list of passwords for archives

For security officers: Getting started with the application web interface

- Kaspersky Anti Targeted Attack Platform Interface
- Selecting a tenant 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 data display period in widgets
- Configuring the widget display scale
- Basics of managing "Alerts" type widgets
- Viewing the working condition of modules and components of the program
- Viewing the alert table
- Configuring the alert table display
- 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 TAA alerts
- Recommendations for processing SB alerts
- Recommendations for processing IOC alerts
- Recommendations for processing YARA alerts
- Recommendations for processing IDS alerts

User actions performed on alerts
- Assigning alerts to a specific 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 source code mode
- Searching events in design mode
- Sorting events in the table
- 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 TAA (IOA) rule based on event search conditions

Event information
- Viewing the table of events
- Configuring the event table display
- 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 "Process terminated" 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 modified" event
- Information about the "System event log" 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 "AMSI scan" 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
Configuring the display of the table of hosts with the Endpoint Agent component
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
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
Automatically sending files from Kaspersky Endpoint Agent hosts to be scanned by the Sandbox component in accordance with Kaspersky TAA (IOA) rules
Enabling and disabling the automatic sending of files from Kaspersky Endpoint Agent hosts to be scanned by the Sandbox component
Managing tasks
Viewing the task table
Viewing information about a task
Creating a get file task
Creating a forensic collection task
Creating a registry key retrieval task
Creating an NTFS metafile retrieval task
Creating a process memory dump retrieval task
Creating a disk image retrieval task
Creating a RAM dump retrieval task
Creating a process termination task
Creating a task to scan hosts using YARA rules
Creating a service management task
Creating a program execution 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
- Configuring prevention rule table display
- Viewing a prevention rule
- Creating a prevention rule
- Importing prevention rules
- 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 hosts
  - Deleting an IOC file
  - Searching for alerts in IOC scan results
  - Searching for events 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
  - Creating a TAA (IOA) rule based on event search conditions
  - Importing a TAA (IOA) rule
  - Viewing custom TAA (IOA) rule details
  - Searching for alerts and events in which TAA (IOA) rules were triggered

Filtering and searching TAA (IOA) rules
Resetting the TAA (IOA) rule filter
Enabling and disabling TAA (IOA) rules
Modifying a TAA (IOA) rule
Deleting 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 user-defined YARA rules
Viewing the YARA rule table
Importing YARA rules
Configuring YARA rule table display
Viewing YARA rule details
Filtering and searching YARA rules
Clearing a YARA rule filter
Enabling and disabling 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 using the web interface
Viewing information about an object placed in Storage by a get file task
Viewing information about an object placed in Storage by a get data 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 type
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
Viewing the table of templates and reports
Creating a template
Creating a report based on a template
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
Managing rules for assigning the VIP status to alerts
Viewing the table of VIP status assignment rules
Creating 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 list of scan exclusions
Viewing the table of data excluded from the scan
Adding a scan exclusion rule
Deleting a scan exclusion rule
Editing a rule added to scan exclusions
Exporting the list of data excluded from the scan
Filtering rules in the scan exclusion list by criterion
Searching rules in the scan exclusion list by value
Resetting the rule filter in the scan exclusion list
Managing IDS exclusions
Viewing the table of Intrusion Detection rules added to exclusions
Adding an IDS rule to exclusions
Editing the description of an IDS rule added to exclusions
Removing an IDS rule from exclusions

- Managing TAA exclusions
  - Viewing the table of TAA (IOA) rules added to exclusions
  - Adding a TAA (IOA) rule to exclusions
  - Viewing a TAA (IOA) rule added to exclusions
  - Removing a TAA (IOA) rule from exclusions
- Creating a list of passwords for archives
- Viewing server settings
- Viewing the table of servers with the Sandbox component
- Viewing the table of servers with the Sensor component
- Viewing the table of external systems

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 Kaspersky Endpoint Agent for Windows
- Installing and uninstalling Kaspersky Endpoint Agent
  - Preparing for Kaspersky Endpoint Agent installation
  - Installing Kaspersky Endpoint Agent
  - Installing and uninstalling Kaspersky Endpoint Agent locally
    - Installing Kaspersky Endpoint Agent using the Installation Wizard
    - Removing Kaspersky Endpoint Agent using the Installation and Uninstallation Wizard
    - Installing, restoring and uninstalling the application using the command line
  - Installing Kaspersky Endpoint Agent using Kaspersky Security Center
    - Creating Kaspersky Endpoint Agent installation package
    - Creating Kaspersky Endpoint Agent remote installation task
  - Installing Kaspersky Endpoint Agent administration tools
    - Installing and updating Kaspersky Endpoint Agent Management plug-in
    - Installing and updating Kaspersky Endpoint Agent Management web plug-in
  - Updating Kaspersky Endpoint Agent from the previous version
  - Repairing Kaspersky Endpoint Agent
  - Changes in the system after Kaspersky Endpoint Agent installation
- 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
Opening Kaspersky Endpoint Agent settings window
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 usage in Kaspersky Endpoint Agent
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
Configuring EDR telemetry settings
Enabling and configuring exclusions for and optimization of sent EDR telemetry about application processes
Enabling and configuring exclusions for sent EDR telemetry about network communications
Configuring storage 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
Configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response
Configuring failure diagnosis
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 tasks manually
Starting tasks by schedule
Viewing task execution results
Configuring the storage time for the task execution results on the Administration Server
Creating Kaspersky Endpoint Agent activation task
Managing Kaspersky Endpoint Agent database and module 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 Kaspersky Endpoint Agent using Kaspersky Security Center Web Console
Managing Kaspersky Endpoint Agent policies
Creating Kaspersky Endpoint Agent policy
Enabling settings in Kaspersky Endpoint Agent policy
Configuring Kaspersky Endpoint Agent settings
Opening Kaspersky Endpoint Agent settings window
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 Kaspersky Endpoint Agent policy type
Configuring KSN usage in Kaspersky Endpoint Agent
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
Configuring EDR telemetry settings
Enabling and configuring exclusions for and optimization of sent EDR telemetry about application processes
Enabling and configuring exclusions for sent EDR telemetry about network communications
Configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response
Configuring storage 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
Configuring failure diagnosis
Managing Kaspersky Endpoint Agent tasks
Creating tasks
Viewing the table of tasks
Deleting a task from the list
Configuring task schedule settings
Starting tasks manually
Creating Kaspersky Endpoint Agent activation tasks
Configuring Database and application module update task
Managing Standard IOC Scan tasks
Requirements for IOC files
Supported IOC terms
Configuring Standard IOC Scan task
Viewing IOC Scan task execution results
Configuring the Quarantine file task
Configuring the Delete file task

Configuring the Run process task
Configuring the Terminate process task
Managing Kaspersky Endpoint Agent using the command line interface
Managing Kaspersky Endpoint Agent activation
Managing Kaspersky Endpoint Agent authentication
Configuring tracing
Configuring creating a dump of Kaspersky Endpoint Agent processes
Viewing information about quarantine settings and quarantined objects
Actions on quarantined objects
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 Standard IOC Scan tasks
Managing scanning of files and processes according to YARA rules
Managing scanning of autorun point objects according to YARA rules
Creating a memory dump
Creating a disk dump
Managing Kaspersky Endpoint Agent for Linux
Installing and removing Kaspersky Endpoint Agent for Linux
Preparing to install Kaspersky Endpoint Agent for Linux
Installing Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Administration Console
Installing the Kaspersky Endpoint Agent for Linux administration plug-in
Adding devices for installing Kaspersky Endpoint Agent for Linux
Creating an installation package for Kaspersky Endpoint Agent for Linux
Remote installation of Kaspersky Endpoint Agent for Linux on selected devices
Installing Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console
Installing the Kaspersky Endpoint Agent web administration plug-in
Adding devices for installing Kaspersky Endpoint Agent for Linux
Creating an installation package for Kaspersky Endpoint Agent for Linux
Remote installation of Kaspersky Endpoint Agent for Linux on selected devices
Local installation of Kaspersky Endpoint Agent for Linux
Updating and restoring Kaspersky Endpoint Agent for Linux
Removing Kaspersky Endpoint Agent for Linux
Managing Kaspersky Endpoint Agent for Linux policies using Kaspersky Security Center Administration Console
Managing policies of Kaspersky Endpoint Agent for Linux
Creating a policy for Kaspersky Endpoint Agent for Linux
Enabling options in the policy of Kaspersky Endpoint Agent for Linux
Managing database and module update tasks for Kaspersky Endpoint Agent
Managing Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console
Managing policies of Kaspersky Endpoint Agent for Linux
Creating a policy for Kaspersky Endpoint Agent for Linux
Enabling options in the policy of Kaspersky Endpoint Agent for Linux
Managing database and module update tasks for Kaspersky Endpoint Agent

Managing Kaspersky Endpoint Agent for Linux using the command line
Verifying the integrity of Kaspersky Endpoint Agent for Linux components
Creating a backup copy and restoring the program from backup
Creating a backup copy of Central Node server settings from the program administrator menu
Downloading a file containing a backup copy of server settings from the Central Node or PCN server to the hard drive of the computer
Uploading a file containing a backup copy of server settings from your computer to the Central Node server
Restoring server settings from a backup copy using 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
Updating Kaspersky Anti Targeted Attack Platform
Upgrading Central Node installed on a server
Contents and amount of information kept when updating Kaspersky Anti Targeted Attack Platform
Interaction with external systems via API
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 that external systems can use to receive information about application alerts
Request to display alert information
Scope of transmitted data
Data on detected objects
Data on detected threats
Data on the environment of detected objects
API for managing Threat Response actions
Request for getting the list of hosts with the Endpoint Agent component
Request for information about network isolation and the existence of prevention rules for hosts with the Kaspersky Endpoint Agent component
Host network isolation management
Request to enable network isolation
Request to disable network isolation
Request to add an exclusion to a network isolation rule
Managing prevention rules
Request to create a prevention rule
Request to delete a prevention rule
Managing the application run task
Request to obtain information about a task
Request to create a task
Request to delete a task
Sources of information about the program
Contacting the Technical Support Service
Obtaining information about Kaspersky Endpoint Agent for Linux for Technical Support
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-файл
- 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
- Kerberos authentication
- Keytab file
- Local reputation database of KPSN
- Malicious web addresses
- MIB (Management Information Base)
- MITM attack
- MITRE technique
- Multitenancy
- New generation threats
- NTP server
- OpenIOC
- Phishing URL addresses
- Sandbox
- Sensor
- Service principal name (SPN)
- SIEM system
- Signature
- SPAN
- Syslog
- Targeted attack
- Targeted Attack Analyzer
- Tenant
- TLS encryption

YARA
YARA rules
Zero-day attack
Zero-day vulnerability
Зеркалированнный трафик
Правило TAA (IOA)
Статус VIP
Трассировка
Information about third-party code
Trademark notices

Kaspersky Anti Targeted Attack Platform Help

New functions

- What's new in the Kaspersky Anti Targeted Attack Platform

Hardware and software requirements

- Hardware and software requirements for computers to work with the program through the web interface
- Compatibility of the Kaspersky Anti Targeted Attack Platform with the Kaspersky Endpoint Agent for Windows and Linux

Licensing

- Licensing the Kaspersky Anti Targeted Attack Platform

Getting started

- Distributed solution and multitenancy
- Sizing the Kaspersky Anti Targeted Attack Platform
- Installation and initial configuration of the Kaspersky Anti Targeted Attack Platform
- Configuring the integration of Kaspersky Anti Targeted Attack Platform with Kaspersky Endpoint Agent

Getting started in the Kaspersky Anti Targeted Attack Platform web interface

- Getting started in the web interface of the program - For an administrator
- Getting started in the web interface of the program - For a security officer

Additional features

- Managing the Sandbox component through the web interface
- Managing Kaspersky Endpoint Agent for Windows
- Managing Kaspersky Endpoint Agent for Linux
- Interaction with external systems via API

Update

- Updating the previous version of the Kaspersky Anti Targeted Attack Platform

Contacting the Technical Support Service

- How to obtain Technical Support

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.

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 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 programs.
- Integrate with Kaspersky Endpoint Agent and receive data from individual computers running Microsoft® Windows® and Linux® operating systems in the corporate IT infrastructure. Kaspersky Endpoint Agent continuously monitors processes running, active network connections, and files that are being modified on those computers.
- 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 programs to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.
- Integration with Kaspersky Private Security Network (KPSN) 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 the results of work done in the web interface of the Central Node, Primary Central Node (hereinafter also PCN) or Secondary Central Node (hereinafter also SCN) servers.
- 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.

Users with the **Senior security officer** or **Security officer** role 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 events 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 the list of VIP alerts and the list of data excluded from the scan, and populate the local reputation database of KPSN.

Users with the **Security auditor** role can perform the following actions in the program:

- Monitor program performance.
- View the table of detected signs of targeted attacks and intrusions into the enterprise IT infrastructure, filter and search alerts, and view the data of each alert.
- Look through the table of events occurring on the computers and servers of the enterprise IT infrastructure, search for threats, filter and view each event.
- View the list of hosts with the Endpoint Agent component and information about selected hosts.
- View the custom rules for Targeted Attack Analyzer TAA (IOA), Intrusion Detection System (IDS), and YARA.
- View the scan-excluded TAA (IOA) rules and IDS rules defined by Kaspersky experts.
- View reports on program performance and reports on alerts.
- View the list of VIP alerts and the list of data excluded from the scan.
- Monitor program performance.
- View all settings made in the program web interface.

Users with the **Local administrator** or **Administrator** role can perform the following actions in the program:

- Configure program operation settings.
- Configure servers for the distributed solution and multitenancy mode.
- 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.

What's new

Kaspersky Anti Targeted Attack Platform now includes the following new functionality and fixes:

1. The Central Node component can be deployed as a fault-tolerant cluster that consists of 2 server roles: storage servers and processing servers. Fault tolerance is achieved through duplication of data between the storage servers and the redundancy of computing resources: if one server fails, its functions are performed by another server with the same role. Meanwhile, the program continues to work.

2. The ability to configure the sizing settings of the program was added. You can specify the planned volume of SPAN traffic, mail traffic, the number of hosts with Kaspersky Endpoint Agent, as well as the planned size of the Storage and event database. The program configures the servers with the Central Node component in accordance with the specified settings.

   A separate web interface is used to configure the sizing settings, called *the web interface for sizing management*. If the Central Node component is deployed as a cluster, you can also view the list of servers and shut down the cluster using the web interface for sizing management.

3. For the Sandbox component, installation of the Astra Linux 1.7 operating system and running objects in this operating system is supported.

   Using an operating system is optional: you can select a set of operating systems that will be used to generate object scan tasks for the Sandbox component: Windows XP, Windows 7, Windows 10; Windows XP, Windows 7, Windows 10, CentOS 7.8 or Windows XP, Windows 7, Windows 10, Astra Linux 1.7.

   The program can run the following objects in Astra Linux 1.7:

   - Files from Kaspersky Endpoint Agent hosts sent to be scanned by the Sandbox component in accordance with Kaspersky TAA (IOA) rules.
   - Files uploaded to Storage manually or by the **Get file** task (if that specific object was sent to be scanned).
   - Files received from mail or network traffic.

4. New task functionality for hosts with the Kaspersky Endpoint Agent for Windows component:

   - The task **Get disk image** was added.

     This task lets you get a disk image of the selected host.

- The task **Get memory dump** was added.

  This task lets you get a RAM dump of the selected host.

  The files resulting from the tasks are saved to a shared network resource.

Adding new task types resulted in the following changes in the program:

- Data collection tasks are now grouped in the **Get data** submenu.
- Renamed task types:
  - **Get file** → **File**.
  - **Collect data** → **Forensics**.
  - **Get registry key** → **Registry key**.
  - **NTFS metafiles** → **NTFS metafiles**.
  - **Get process memory dump** → **Process memory dump**.

5. New event type added: **Process terminated**.
6. The program web interface is changed in the following ways:
   - In the network interface settings window, the option to choose how to configure this interface has been added: manually or import settings from a DHCP server.
   - The option to disable synchronization with an NTP-server was removed from the Settings section, subsection Date and time.
   - The option to enter the maximum allowed hard disk space usage for Central Node and Sensor servers was removed.

Kaspersky Endpoint Agent for Windows 3.14 now includes the following new functionality and fixes:

1. Now you can interact with the fault-tolerant clusters of Kaspersky Anti Targeted Attack Platform servers.
2. Now you can create a full memory and a full disk dump of a protected device through the command line interface for further use of Kaspersky Anti Targeted Attack Platform.
3. Introduced Kaspersky Endpoint Agent operation mode in which the program is compatible with Azure WVD.
4. An error related to the possible blocking of files processed by Kaspersky Endpoint Agent is fixed.

Kaspersky Endpoint Agent 3.12 for Linux has the following changes:

Managing the Kaspersky Managed Detection and Response solution is no longer supported. It is not recommended to use Kaspersky Endpoint Agent for Linux to work with this solution. To work with Kaspersky Managed Detection and Response, use Kaspersky Endpoint Security for Linux.

Using 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 for a fee. Authorization on the application website requires that an application access certificate is installed in the certificate storage on your computer. In addition, you must have a user name and password for access to the application.

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 Ubuntu® Server 20.04.5 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 7.9 operating system and for the Sandbox component.
3. Disk images (files with the .iso extension) of the Windows XP SP3, Windows 7 (64-bit), Windows 10 (64-bit), and CentOS 7.8 operating systems that the Sandbox component will use for running files.

   For Russian users, a disk image with the Astra Linux 1.7 operating system is also supplied.
4. The kata-upgrade-preparation script for updating the Central Node component.
5. 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.

File	Description
agent\klcfginst.msi	Installation package for Kaspersky Endpoint Agent Management administration 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.
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 application over the web interface:

- Mozilla™ Firefox™ for Linux.
- Mozilla Firefox for Windows.
- Google™ Chrome™ for Windows.
- Google Chrome for Linux.
- Edge (Windows).
- Safari (Mac).

Minimum screen resolution to use web interface: 1366x768.

Deploying the application on a virtual platform requires installing the VMware ESXi™ hypervisor version 6.7.0 or 7.0.

> For the application to work correctly in a virtual environment, you must install an up-to-date patch for the hypervisor.

The configuration of the servers hosting the Central Node, Sandbox and Sensor components depends on the volume of data processed by the application 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 for Windows

This section describes hardware and software requirements of Kaspersky Endpoint Agent 3.14 for Windows.

If the version of Kaspersky Anti Targeted Attack Platform on the Central Node servers is incompatible with the version of Kaspersky Endpoint Agent 3.14 for Windows that is installed on the computers of the corporate LAN, the functionality of Kaspersky Anti Targeted Attack Platform may be limited.

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

Software requirements for installing Kaspersky Endpoint Agent 3.14 for Windows

Supported operating systems for workstations:

- Windows 7 SP1 Home / Professional / Enterprise / Ultimate 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 19H1 (version 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 (version 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 (version 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H2 (version 2009) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H1 (version 21H1) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 21H2 (version 21H2) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 11 21H2 (version 21H2) Home / Professional / Education / Enterprise 32-bit / 64-bit

Supported server operating systems:

- Windows Server 2008 SP2 Standard / Enterprise 64-bit
- Windows Server 2008 R2 SP1 Foundation / Standard / Enterprise 64-bit

- Windows Server 2012 Foundation / Standard / Enterprise / Datacenter 64-bit
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-bit
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit
- Windows Server 2019 Essentials / Standard / Datacenter 64-bit
- Windows Server 20H2 Standard Core / Datacenter Core 64-bit
- Windows Server 2022 Standard / Datacenter 64-bit

Supported embedded operating systems:

- Windows Embedded Standard 7 SP1 32-bit / 64-bit.

Software requirements for installing Kaspersky Endpoint Agent 3.14 for Windows when integrating with Kaspersky Industrial CyberSecurity for Nodes

Supported operating systems for workstations:

- Windows XP Professional SP2 32-bit / 64-bit.
- Windows XP Professional SP3 32-bit.
- Windows Vista SP2 32-bit / 64-bit.
- Windows 7 SP1 Home / Pro / Enterprise / Ultimate 32-bit / 64-bit.
- Windows 8 Pro / Enterprise 32-bit / 64-bit.
- Windows 8.1 Pro / Enterprise 32-bit / 64-bit.
- Windows 10 LTSC 2015 (1507) 32-bit / 64-bit.
- Windows 10 LTSC 2016 (1607) 32-bit / 64-bit.
- Windows 10 LTSC 2019 (1809) 32-bit / 64-bit.
- Windows 10 LTSC 2021 (21H2) 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 1703 RS2 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 1803 RS4 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 1809 RS5 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 1903 19H1 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 1909 19H2 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 2004 20H1 32-bit / 64-bit.

- Windows 10 Home / Pro / Education / Enterprise 2009 20H2 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 21H1 32-bit / 64-bit.
- Windows 10 Home / Pro / Education / Enterprise 21H2 32-bit / 64-bit.

Supported server operating systems:

- Windows Server 2003 SP1 Standard / Enterprise / Datacenter 32-bit / 64-bit.
- Windows Server 2003 SP2 Standard / Enterprise / Datacenter 32-bit / 64-bit.
- Windows Server 2008 SP2 Standard / Enterprise / Datacenter 32-bit / 64-bit.
- Windows Server 2003 R2 Standard / Enterprise / Datacenter 32-bit / 64-bit.
- Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter 32-bit / 64-bit.
- Windows Server 2012 Foundation / Standard / Essentials / Datacenter 64-bit.
- Windows Server 2012 R2 Foundation / Standard / Enterprise / Datacenter 64-bit.
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit, versions 1709 and 1803.
- Windows Server 2019 Standard Core / Datacenter Core 64-bit, versions 1903, 1909, 2004, 20H2, and 21H2.

Supported embedded operating systems:

- Windows XP Embedded SP2 (WEPOS) 32-bit / 64-bit.
- Windows XP Embedded SP3 (POSReady 2009) 32-bit.
- Windows 7 SP1 Embedded (POSReady 7) 32-bit / 64-bit.
- Windows Embedded 8.1 Industry Pro 32-bit / 64-bit.
- Windows 10 IoT Enterprise 32-bit / 64-bit versions 1703, 1803, 1809, 1903, 1909, 2004, 2009, 21H1, and 21H2.

When creating an installation package in Kaspersky Security Center version 12 or later to install Kaspersky Endpoint Agent on Windows XP devices, you must use the installer file (setup.exe) from the installation package created in Kaspersky Security Center version 10.5.

Hardware requirements for installing Kaspersky Endpoint Agent 3.14 for Windows

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 Kaspersky Endpoint Security, the Kaspersky Anti Targeted Attack Platform has limited functionality if the Windows Server® 2008 SP2 64-bit operating system is installed on the Kaspersky Endpoint Security server.

To manage Kaspersky Endpoint Agent using the Kaspersky Security Center Web Console, you need Google Chrome for Windows.

Compatibility of Kaspersky Endpoint Agent for Windows 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 Kaspersky Anti Targeted Attack Platform 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.

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

Compatibility of Kaspersky Endpoint Agent for Windows versions with Kaspersky Anti Targeted Attack Platform versions

Version Kaspersky Endpoint Agent	Type Kaspersky Endpoint Agent	Compatibility with KATA 3.7	Compatibility with KATA 3.7.1	Compatibility with KATA 3.7.2	Compatibility with KATA 4.0	Compatibility with KATA 4.1	Compatibility with KATA 5.0
Endpoint Agent 3.7	Standalone installation or as part of KES versions 11.2 and 11.3	No	No	No	No	No	No
Endpoint Agent 3.8	Standalone installation	Yes	Yes	There are limitations	There are limitations	There are limitations	There are limitations
Endpoint Agent 3.9	Standalone installation or as part of EPP applications	Yes	Yes	There are limitations	There are limitations	There are limitations	There are limitations
Endpoint Agent 3.10	Standalone installation or as part of EPP applications	No	There are limitations	Yes	There are limitations	There are limitations	There are limitations
Endpoint Agent 3.11	Standalone installation or as part of KES version 11.7	No	There are limitations	Yes	There are limitations	There are limitations	There are limitations

Version Kaspersky Endpoint Agent	Type Kaspersky Endpoint Agent	Compatibility with KATA 3.7	Compatibility with KATA 3.7.1	Compatibility with KATA 3.7.2	Compatibility with KATA 4.0	Compatibility with KATA 4.1	Compatibility with KATA 5.0
Endpoint Agent 3.12	Standalone installation	No	No	No	Yes	There are limitations	There are limitations
Endpoint Agent 3.13	Standalone installation	No	No	No	There are limitations	Yes	There are limitations
Endpoint Agent 3.14	Standalone installation	No	No	No	There are limitations	There are limitations	Yes

Compatibility of Kaspersky Endpoint Agent for Windows versions with EPP applications

You can use Kaspersky Endpoint Agent alone or set up an integration of Kaspersky Endpoint Agent with workstation protection programs (Endpoint Protection Platform, hereinafter also "EPP"), Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Server, and Kaspersky Security for Virtualization Light Agent. If the integration of programs is configured, Kaspersky Endpoint Agent also sends the information about threats detected by EPP programs and their processing results to the Central Node server.

The integration scenarios described above do not work when Kaspersky Endpoint Agent is installed on a virtual desktop in Virtual Desktop Infrastructure.

Integration of Kaspersky Endpoint Agent with Kaspersky Endpoint Security for Windows and Kaspersky Security for Windows Server requires installing Kaspersky Endpoint Agent as part of those programs.

Compatibility of Kaspersky Endpoint Agent for Windows with versions of Kaspersky Security for Windows Server

You can install the following versions of Kaspersky Endpoint Agent as part of Kaspersky Security for Windows Server:

- Kaspersky Endpoint Agent 3.9 as part of Kaspersky Security 11 for Windows Server.
- Kaspersky Endpoint Agent 3.10 as part of Kaspersky Security 11.0.1 for Windows Server.

When you install Kaspersky Endpoint Agent as part of Kaspersky Security for Windows Server, the standalone Kaspersky Endpoint Agent of the same or earlier version is removed. If Kaspersky Endpoint Agent installed as part of Kaspersky Security for Windows Server has an earlier version, it will not be installed. In this case, you must first remove the standalone Kaspersky Endpoint Agent.

If necessary, you can upgrade the Kaspersky Endpoint Agent that is already installed as part of Kaspersky Security for Windows Server. Integration between compatible versions of the programs is maintained both when Kaspersky Endpoint Agent is upgraded and when Kaspersky Security for Windows Server is upgraded.

Information about the compatibility of Kaspersky Endpoint Agent versions with Kaspersky Security for Windows Server versions is listed in the table below.

Compatibility of Kaspersky Endpoint Agent versions with Kaspersky Security for Windows Server versions

Kaspersky Security for Windows Server version	Compatibility with Endpoint Agent 3.8, 3.9, 3.10	Compatibility with Endpoint Agent 3.11, 3.12	Compatibility with Endpoint Agent 3.13, 3.14
• KSWS 10.1.2	Yes	No	No
• KSWS 11	Yes	Yes	No
• KSWS 11.0.1	No	Yes	Yes

For more details about installing Kaspersky Security for Windows Server, see *Kaspersky Security for Windows Server Help*.

Compatibility of Kaspersky Endpoint Agent for Windows with versions of Kaspersky Endpoint Security for Windows

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

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

  Kaspersky Endpoint Agent (Endpoint Sensors) 3.6.1 is not compatible with Kaspersky Anti Targeted Attack Platform version 4.1 or later.

  Kaspersky Endpoint Agent 3.7 is incompatible with all versions of 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.
- Kaspersky Endpoint Agent 3.11 as part of Kaspersky Endpoint Security 11.7, 11.8.

When you install Kaspersky Endpoint Agent 3.10 or later as part of Kaspersky Endpoint Security for Windows, the standalone Kaspersky Endpoint Agent program of the same or earlier version is removed. If the separately installed Kaspersky Endpoint Agent has a later version, the program bundled with Kaspersky Endpoint Security for Windows is not installed. In this case, you must first remove the standalone Kaspersky Endpoint Agent.

If necessary, you can upgrade the Kaspersky Endpoint Agent that is already installed as part of Kaspersky Endpoint Security for Windows. Integration between compatible versions of the programs is maintained when both Kaspersky Endpoint Agent is updated and when Kaspersky Endpoint Security for Windows is updated. You can upgrade a previous version of Kaspersky Endpoint Agent to version 3.14 only for Kaspersky Endpoint Agent version 3.7 or later.

Information about the compatibility of Kaspersky Endpoint Agent versions with Kaspersky Endpoint Security for Windows versions is listed in the table below.

Compatibility of Kaspersky Endpoint Agent versions with Kaspersky Endpoint Security for Windows versions

Kaspersky Endpoint Security version	Compatibility with Endpoint Agent 3.8, 3.9	Compatibility with Endpoint Agent 3.10, 3.12	Compatibility with Endpoint Agent 3.11	Compatibility with Endpoint Agent 3.13, 3.14
• KES 10 SP2 MR2	No	No	No	No
• KES 10 SP2 MR3/MR4	Yes	No	No	No
• KES 11.0.0	No	No	No	No
• KES 11.0.1	Yes	No	No	No
• KES 11.1 • KES 11.1.1	Yes	Yes	No	No
• KES 11.2 • KES 11.3	Yes	Yes	Yes	No
• KES 11.4 • KES 11.5	Yes	Yes	Yes	No
• KES 11.6–11.12 • KES 11.14–11.18	Yes	Yes	Yes	Yes
• KES 11.13	No	No	No	Yes

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

Compatibility of Kaspersky Endpoint Agent with versions of Kaspersky Security for Virtualization Light Agent

You can configure the integration of separately installed Kaspersky Endpoint Agent and Kaspersky Security for Virtualization Light Agent.

Information about the compatibility of Kaspersky Endpoint Agent versions with Kaspersky Security for Virtualization Light Agent is listed in the table below.

Compatibility of Kaspersky Endpoint Agent versions and Kaspersky Security for Virtualization Light Agent versions

Kaspersky Security for Virtualization Light Agent version	Compatibility with Endpoint Agent 3.8, 3.9, 3.10	Compatibility with Endpoint Agent 3.12	Compatibility with Endpoint Agent 3.11, 3.13, 3.14
• KSV 5.1 LA	Yes	Yes	No
• KSV 5.1.1 LA	Yes	No	No
• KSV 5.2 LA	No	Yes	Yes

Kaspersky Endpoint Agent and Kaspersky Security for Virtualization Light Agent installed on a virtual machine generate the same load on the Central Node server as Kaspersky Endpoint Agent and Kaspersky Security for Virtualization Light Agent installed on the host.

For more details about enabling the integration of Kaspersky Endpoint Agent with Kaspersky Security for Virtualization Light Agent, see *Kaspersky Security for Virtualization Light Agent Help*.

Compatibility of Kaspersky Endpoint Agent with versions of Kaspersky Industrial CyberSecurity for Nodes

You can install Kaspersky Endpoint Agent on a device with Kaspersky Industrial CyberSecurity for Nodes installed. The applications are integrated automatically.

Integration is supported only for Kaspersky Endpoint Agent version 3.14 and Kaspersky Industrial CyberSecurity for Nodes version 3.1. Integration between other versions of the programs is not supported.

To integrate with Kaspersky Industrial CyberSecurity for Nodes, the corresponding license key must be installed in the Kaspersky Endpoint Agent.

For detailed information, you can contact your account manager.

Compatibility of Kaspersky Endpoint Agent for Windows versions with other applications

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

Compatibility of Kaspersky Endpoint Agent 3.8 and 3.9 for Windows 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, or later.
- Kaspersky Sandbox 1.0.

Compatibility of Kaspersky Endpoint Agent 3.8 and 3.9 for Windows with third-party anti-virus programs

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

- Symantec™ Endpoint Protection.
- Sophos Endpoint Protection.

- ESET NOD32™ Business Edition Smart Security.
- Bitdefender® GravityZone® Advanced Business Security.
- McAfee® Endpoint Security 10.6.1.
- McAfee® Endpoint Security 10.7.

If multiple third-party anti-virus programs are simultaneously installed on the computer, correct operation of Kaspersky Endpoint Agent is not guaranteed.

If RealTimes Desktop Service is installed on computers on which you want to install Kaspersky Endpoint Agent, you are advised to remove it before installing Kaspersky Endpoint Agent.

Compatibility of Kaspersky Endpoint Agent for Windows version 3.10 with other Kaspersky programs

Kaspersky Endpoint Agent version 3.10 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center versions 11 and 12.1.
- Kaspersky Sandbox 1.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Compatibility of Kaspersky Endpoint Agent 3.10 for Windows with third-party anti-virus programs

Computers on which you want to install Kaspersky Endpoint Agent 3.10 can have Bitdefender GravityZone Advanced Business Security installed.

Compatibility of Kaspersky Endpoint Agent for Windows version 3.11 with other Kaspersky programs

Kaspersky Endpoint Agent version 3.11 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center 10.5, 11, 12.1, 13, or later.
- Kaspersky Sandbox 1.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.
- Kaspersky Industrial CyberSecurity for Networks 3.0.

Compatibility of Kaspersky Endpoint Agent 3.11 for Windows with third-party anti-virus programs

Computers on which you want to install Kaspersky Endpoint Agent 3.11 can have Bitdefender GravityZone Advanced Business Security installed.

Compatibility of Kaspersky Endpoint Agent 3.12 for Windows with other Kaspersky programs

Kaspersky Endpoint Agent 3.12 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center versions 13, 13.1, and 13.2.
- Kaspersky Security Center Cloud Console.
- Kaspersky Sandbox 1.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Compatibility of Kaspersky Endpoint Agent for Windows versions 3.13 and 3.14 with other Kaspersky programs

Kaspersky Endpoint Agent versions 3.13 and 3.14 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center versions 13, 13.1, 13.2, and 14.
- Kaspersky Sandbox 2.0.
- Kaspersky Endpoint Detection and Response Optimum 1.0.

Requirements for Kaspersky Endpoint Agent for Linux

This section describes hardware and software requirements of Kaspersky Endpoint Agent 3.12 for Linux.

Software requirements for installing Kaspersky Endpoint Agent 3.12 for Linux

Kaspersky Endpoint Agent 3.12 only works on computers that have one of the following operating systems installed:

- Ubuntu® 16.04 LTS or later
- Ubuntu 18.04 LTS or later
- Ubuntu 20.04 LTS
- Red Hat® Enterprise Linux® 7.2 or later
- Red Hat Enterprise Linux 8.0 or later
- CentOS 7.2 or later
- CentOS 8.0 or later
- Debian GNU / Linux 9.4 or later
- Debian GNU / Linux 10.1 or later
- Debian GNU / Linux 11 or later
- Oracle® Linux 7.3 or later
- Oracle Linux 8 or later
- SUSE Linux Enterprise Server 12 or later
- SUSE Linux Enterprise Server 15
- Astra Linux Special Edition RUSB.10015-01 (regular update 1.6)
- Astra Linux Special Edition RUSB.10015-01 (regular update 1.7)
- Astra Linux Special Edition RUSB.10015-16 (variant 1) (regular update 1.6)
- Astra Linux Common Edition (regular update 2.12)
- Alt 8 SP Server
- Alt Server 9
- Alt Workstation 9
- Goslinux 7.17
- RED OS 7.3

Hardware requirements for installing Kaspersky Endpoint Agent 3.12 for Linux

Minimum hardware requirements:

- CPU: 2 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Required software

Kaspersky Endpoint Agent for Linux requires Linux Audit Daemon 2.8 or later. Installed on hosts with Kaspersky Endpoint Agent.

Compatibility of Kaspersky Endpoint Agent 3.12 for Linux with Kaspersky EPP programs

Kaspersky Endpoint Agent 3.12 supports integration with Kaspersky Endpoint Security for Linux 11.1, 11.2.

Compatibility of Kaspersky Endpoint Agent 3.12 for Linux with other Kaspersky programs

Kaspersky Endpoint Agent 3.12 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center 13, 13.2.
- Kaspersky Endpoint Agent administration plug-in 3.10, 3.11, 3.12.
- Kaspersky Endpoint Agent web plug-in 3.10, 3.11, 3.12.

Compatibility of Kaspersky Endpoint Agent for Linux versions with Kaspersky Anti Targeted Attack Platform versions

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

Compatibility of Kaspersky Endpoint Agent for Linux versions with Kaspersky Anti Targeted Attack Platform versions

Version of Endpoint Agent	Type of Endpoint Agent	Compatibility with KATA 3.6.1	Compatibility with KATA 3.7, 3.7.1	Compatibility with KATA 3.7.2	Compatibility with KATA 4.0	Compatibility with KATA 4.1, 5.0
Endpoint Agent 3.9	Standalone installation or part of KES version 11.1	No	No	Yes	Yes	No
Endpoint Agent 3.12	Standalone installation	No	No	Yes	Yes	Yes

Compatibility of Kaspersky Endpoint Agent for Linux versions with EPP applications

You can use Kaspersky Endpoint Agent alone or configure the integration of Kaspersky Endpoint Agent with the workstation protection program (Endpoint Protection Platform, hereinafter also called EPP) Kaspersky Endpoint Security for Linux. If the integration is configured, Kaspersky Endpoint Agent also sends the information about threats detected by this program and the results of threat processing to the Central Node server.

Kaspersky Endpoint Agent 3.9 and 3.12 are compatible with the following versions of Kaspersky Endpoint Security for Linux: 11.1, 11.2.

For more details about installing Kaspersky Endpoint Security, see *Kaspersky Endpoint Security for Linux Help*.

Compatibility of Kaspersky Endpoint Agent for Linux versions with other applications

Compatibility of Kaspersky Endpoint Agent 3.9 for Linux with other Kaspersky programs

Kaspersky Endpoint Agent 3.9 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center versions 12.1 and 12.2.
- Kaspersky Endpoint Agent administration plug-in 3.10.
- Kaspersky Endpoint Agent web plug-in 3.10.

Compatibility of Kaspersky Endpoint Agent 3.12 for Linux with other Kaspersky programs

Kaspersky Endpoint Agent 3.12 can be integrated with the following Kaspersky programs and solutions:

- Kaspersky Security Center 13, 13.2.
- Kaspersky Endpoint Agent administration plug-in 3.10, 3.11, 3.12.
- Kaspersky Endpoint Agent web plug-in 3.10, 3.11, 3.12.

Compatibility of Kaspersky Endpoint Security for Windows versions with Kaspersky Anti Targeted Attack Platform versions

You can use Kaspersky Endpoint Security as the Endpoint Agent component.

Information about the compatibility of Kaspersky Endpoint Security versions with Kaspersky Anti Targeted Attack Platform versions is listed in the table below.

Compatibility of Kaspersky Endpoint Security for Windows versions with Kaspersky Anti Targeted Attack Platform versions

Kaspersky Endpoint Security version	Compatibility with KATA 4.0	Compatibility with KATA 4.1	Compatibility with KATA 5.0	Compatibility with KATA 5.1	Compatibility with KATA 6.0	Compatibility with KATA 6.1	Compatibility with KATA 7.0	Compatibility with KATA 7.1
Kaspersky Endpoint Security 12.1, 12.2	No	Yes	Yes	Yes	Yes	No	There are limitations	There are limitations
Kaspersky Endpoint Security 12.3, 12.4	No	Yes	Yes	Yes	Yes	Yes	There are limitations	There are limitations
Kaspersky Endpoint Security 12.5, 12.6	No	No	Yes	Yes	Yes	Yes	There are limitations	There are limitations
Kaspersky Endpoint Security 12.7	No	No	There are limitations	There are limitations	There are limitations	There are limitations	Yes	There are limitations
Kaspersky Endpoint Security 12.8, 12.9	No	No	There are limitations	There are limitations	There are limitations	There are limitations	There are limitations	Yes
Kaspersky Endpoint Security 12.10, 12.11	No	No	Yes	Yes	Yes	Yes	Yes	Yes

For more information about compatibility limitations of Kaspersky Endpoint Security versions with Kaspersky Anti Targeted Attack Platform versions, see the *Limited compatibility of Kaspersky Endpoint Security for Windows versions with Kaspersky Anti Targeted Attack Platform versions* section.

Starting from version 12.8, Kaspersky Endpoint Security for Windows can be used as the Light Agent for Windows component for the Kaspersky Security for Virtualization application. For more details about the integration, see Kaspersky Security for Virtualization Light Agent Help.

Limitations of the current version of the application

Kaspersky Anti Targeted Attack Platform 5.0 has the following known limitations:

1. When you upgrade to version 5.0, a non fault-tolerant version of the program is installed. The program data is saved during the update process.

2. To update the Central Node component on the server with this component, you must first run the script. The script is included in the program distribution kit.

3. If the Central Node component is installed on a virtual server, before you upgrade the application, make sure that BIOS boot mode is selected for the virtual machine. If EFI boot mode is selected for the virtual machine, an error will occur if you try to install the upgrade.

Restrictions that apply when deploying the Central Node component:

The password for the local administrator account is preset. You can change the password in the web interface of the program.

Restrictions that apply when deploying the Central Node component as a cluster:

1. A Central Node cluster must include at least 4 servers: 2 storage servers and 2 processing servers. You can scale the cluster to increase the amount of traffic handled or the number of connected hosts in accordance with the Sizing Guide.

2. It is recommended to add servers with the same hardware configuration to the cluster. Otherwise, a proportional increase in performance is not guaranteed.

3. Adding an extra server to the cluster does not speed up the processing of objects that are already in the scan queue.

4. The web interface of the program can be unavailable for some time if the server on which it is located fails.

5. If the processing server fails, you may lose ICAP, POP3, and SMTP traffic data as well as the copies of emails that are waiting to be processed and the detections associated with them.

6. If the processing server is configured to receive mirrored traffic from SPAN ports, then SPAN traffic is not processed if this server fails.

7. If one of the cluster servers fails or the connection between the server and the Kaspersky Endpoint Agent program is temporarily lost, temporary data synchronization in the event database is still possible.

8. If the configuration of the cluster servers is changed, traffic and events from hosts with Kaspersky Endpoint Agent may be temporarily slowed down.

Restrictions that apply to the Sandbox component:

If the set of operating systems installed on the Sandbox server does not match the set selected on the Central Node server, Kaspersky Anti Targeted Attack Platform does not send objects to be scanned by the Sandbox server. If multiple Sandbox servers are connected to the Central Node server, the program sends objects to those Sandbox servers whose installed operating systems match the set selected on Central Node.

Limitations that apply when integrating with the Kaspersky Endpoint Agent for Windows:

1. RAM dump retrieval and disk image retrieval tasks can only be assigned to hosts with Kaspersky Endpoint Agent for Windows version 3.14.

2. Tasks for getting process memory dumps, NTFS metafiles, and registry keys can only be assigned to hosts with Kaspersky Endpoint Agent for Windows version 3.13 or later.

3. The task of scanning hosts using YARA rules can only be assigned to hosts with Kaspersky Endpoint Agent for Windows versions 3.12 or later. If you simultaneously assign a task to hosts with Kaspersky Endpoint Agent version 3.12 or later, and to hosts with earlier versions of the program, the task is executed only on hosts with Kaspersky Endpoint Agent 3.12 or later.

   If autorun points are selected as the scan scope, the task is run only on hosts with Kaspersky Endpoint Agent 3.13 or later.

Limitations that apply when integrating with Kaspersky Endpoint Agent 3.12 for Linux:

1. Hosts with Kaspersky Endpoint Agent for Linux program cannot use the following functions:

   - Network isolation of a host.

   - Creating a prevention rule.

     No notifications are created about the unsuccessful application of a prevention rule on hosts with Kaspersky Endpoint Agent for Linux program.

   - Finding indicators of compromise on hosts using IOC files.

     No notifications are created about the unsuccessful search of indicators of compromise on hosts with the Kaspersky Endpoint Agent for Linux program.

2. Searching the event database using the **OSVersion** criterion displays only hosts with the Kaspersky Endpoint Agent for Linux program. Hosts with the Kaspersky Endpoint Agent for Windows program are not displayed in search results.

3. The **OS name** field in the event information is only filled in for events that are logged in the event database by Kaspersky Endpoint Agent for Linux. Event information logged in the event database by Kaspersky Endpoint Agent for Windows does not have this field filled in.

4. The list of events that Kaspersky Endpoint Agent for Linux logs in the event database is limited to the following types:

   - **File modified**.
   - **Process started**.
   - **System event log**.
   - **Scan: detect**.
   - **Scan: detect processing result**.

5. The list of tasks that you can create on hosts with the Kaspersky Endpoint Agent for Linux program is limited to the following types:

   - **Get file**
   - **Run program**

     When you create the task, the program does not attempt to verify the path to the executable file or the file that you want to receive.

6. In information about events registered in the event database by Kaspersky Endpoint Agent for Linux, the **Time created** field displays file modification time.

Kaspersky Endpoint Agent 3.14 for Windows has the following known limitations:

1. SHA-2 support in Windows is required for Kaspersky Endpoint Agent to work correctly.

2. When creating an installation package in Kaspersky Security Center version 12 or later to install Kaspersky Endpoint Agent on Windows XP devices, you must use the installer file (setup.exe) from the installation package created in Kaspersky Security Center version 10.5.

3. In Kaspersky Security Center 13.2 or later, to install Kaspersky Endpoint Agent on Windows XP devices, you must use the standard Kaspersky Endpoint Agent 3.14 distribution kit instead of the installation package created in Kaspersky Security Center.

4. 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.

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

6. 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 program installer and perform recovery in the quiet mode with the REINSTALL=Drivers.klelam key.

7. After installing, restoring, changing set of components, or removing Kaspersky Endpoint Agent, it is recommended to restart the operating system as soon as possible because changes to some program settings can only be finalized at system startup.

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

9. The component that prohibits opening documents has the following limitation: document blocking rules are not applied to objects that are opened using OLE automation.

10. Before sending telemetry events to the KATA Central Node server, Kaspersky Endpoint Agent saves data in the event queue. If the event queue exceeds 10,000 unprocessed events, Kaspersky Endpoint Agent does not queue the events until free slots appear in the queue.

11. If Kaspersky Endpoint Agent is running on devices with the Windows 7 operation system, the program excludes data about network connections related to processes with PID=4 and PID=0 from telemetry.

12. 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.

13. If more than one application is specified as the value of the *Application* criterion when configuring the settings of network isolation exclusions, Kaspersky Endpoint Agent allows connection only for the first application in the list. Network connections for other applications specified in the list will be ignored. This limitation is reproduced when isolating devices with Windows 7 or Windows Server 2008 R2 operating systems.

14. 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 John Smith* by the `is` condition, the indicator description must be specified in the following format: <Content type="string"><![CDATA[Copyright (C) 1998-2017 John Smith]]></Content>. To simplify description of the indicators, the `contains` condition can also be used.

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

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

    Program localization affects the language of texts used to describe program modules in the system and when publishing program 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 program interface of Administration Console (interface of policies, group tasks, and program properties). Configuring the localization of the program manually is not supported.

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

19. After installing, restoring, changing set of components, or removing Kaspersky Endpoint Agent, it is recommended to restart the operating system as soon as possible because changes to some program settings can only be finalized at system startup.

20. If the start schedule for a group task is set to **On application launch**, the task execution status is updated with a delay in the task execution history For this reason, in some cases, the task execution history will not display the task execution statuses.

21. If the operating system is activated under a Volume License, you may need to reactivate the operating system after Kaspersky Endpoint Agent is installed due to the installation of the program network drivers.

22. In the Windows XP and Windows Vista operating systems, some information about files in telemetry events sent to the Telemetry collection server may be missing. This is due to the fact that the possibility of obtaining some information about files appeared in later versions of MS Windows operating systems.

Kaspersky Endpoint Agent 3.12 for Linux has the following known limitations:

1. Kaspersky Endpoint Agent for Linux does not support AppArmor and SELinux mandatory access control systems in their enforcing modes. For the program to work correctly, these systems must be switched to permissive mode.

2. Kaspersky Endpoint Agent for Linux requires installing Linux Audit Daemon 2.8 or later on the device.

3. For connection of Kaspersky Endpoint Agent for Linux with Kaspersky Endpoint Security for Linux rsyslog service with loaded imuxsock module is used. To check if the module is loaded in the rsyslog service configuration, run the following command: grep -r imuxsock /etc/rsyslog*. If the module loading string is commented, remove the # comment sign before the string and restart rsyslog service to save the changes.

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 application).

  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 application distribution kit.

- In the KSN Statement (for example, during installation of the application 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 application 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 perimeter of your organization if a server with the Kaspersky Private Security Network application is located outside of your organization.

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

Service data of the application

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 application installed may be granted access to the personal data of other users.

Information about the service data of Kaspersky Anti Targeted Attack Platform is provided in the table below.

Service data of Kaspersky Anti Targeted Attack Platform

Data type	Location and duration of storage
• Data on user accounts. • Data of the Central Node component. • Data about tenants. • Information about computers connected to the Central Node component on which the Endpoint Agent component is installed. • Data about presets and prevention rules. • Information about tasks assigned to computers with the Endpoint Agent component. • Custom widget layout data. • Information about user-defined TAA (IOA) rules. • Information about user-defined IDS rules. • Information about user-defined IOC rules. • Data on network isolation rules. • Data about scan exclusions. • Information about reports and report templates. • Information about Endpoint Agent component certificates.	Data is stored indefinitely on the server hosting the Central Node component in the `/data` directory if the Central Node component is installed on the server. When the Central Node component is installed on a cluster, data is stored on storage servers indefinitely.

Data type	Location and duration of storage
Information about MDR, KSN, KPSN integration.	The information is stored indefinitely on the Central Node server in the `/data` directory.
Information about applied license keys or activation codes.	
Endpoint Agent settings.	
Settings of the mail server used for sending notifications: • IP address and port of the server. • Fingerprint of the certificate. • Login and password hash of the user authorized on the server. • Name of the secret that is used as the decryption key. • Whether encryption is being used.	
Name of the current server.	
Addresses of servers connected to the current server and information about certificates used for mutual authentication with them.	
Connector settings: • Address of the connector node. • Server address of the third-party system with which the connector interacts.	
Information about secrets and user account information of Central Node users.	
Address of the monitoring point.	
Information about ICAP exclusions.	

Data type	Location and duration of storage
Settings of Sensor integration with ICAP: • State (enabled or disabled). • Maximum number of connections. • Connection address in REQMOD mode. • Connection address in RESPMOD mode. • ICAP request header that contains the IP address of the client that made the HTTP request when this request is received through the proxy server. • ICAP request header that contains the port of the client that made the HTTP request when this request is received through the proxy server. • User name. • ICAP request header that contains the user name of the client that made the HTTP request when this request is received through the proxy server. • Whether base64 decoding was used. • Operating mode. • Scan timeout. • Detection importance. • Page returned to the user when a file is blocked. • Page returned to the user when a URL is blocked. • Interfaces listened on.	
Settings for sending user-defined intrusion detection rules to KSN.	
Information about the state and names of Keytab files used in Kerberos authentication.	
Information about KSMG email message scanning priorities.	
CPU and RAM load notification settings: • CPU, hard drive, and RAM usage thresholds. • Statistics update interval.	
Information about certificates used for mutual authentication of Sensor and Central Node.	
Settings of Sensor integration with POP3: • IP address and port of the POP3 server. • Login and password hash of the user authorized on the POP3 server. • Name of the secret that is used as the decryption key. • Certificate verification policy. • Client certificates.	

Data type	Location and duration of storage
Proxy server settings: • IP address and port of the proxy server. • Login and password hash of the user authorized on the proxy server. • Name of the secret that is used as the decryption key. • State of the proxy server.	
Storage server settings: • Storage size. • Storage duration.	
Settings of Sandbox servers: • IP address and name of the server. • State of the server. • Fingerprint of the certificate.	
Sandbox settings: • List of virtual machine images. • Sandbox synchronization state.	
Security settings: • Password change and reset period. • Failed authentication counter. • Maximum user inactivity time. • **Dashboard** locking state because of user inactivity.	
Settings of Sensor servers: maximum size of a file that can be sent for scanning.	
SIEM settings: • State of local and remote update and action logs. • TLS encryption state. • SIEM server addresses and ports. • Network protocol being used. • ID of the host sending data to SIEM. • TLS encryption certificate.	
Settings of Sensor integration with SMTP: • Certificates used for mutual authentication. • Domain and subdomain names. • SMTP client networks and subnets. • TLS security level. • Status of requesting client TLS certificate. • SMTP state.	
SNMP connection settings: • Login. • Password hash. • Name of the secret that is used as the decryption key. • Protocol version. • SNMP state.	

Data type	Location and duration of storage
Settings of Sensor integration with SPAN: • Interfaces listened on. • State of saving HTTP headers. • SPAN state. • Client certificates.	
Settings of storage for mirrored traffic from SPAN ports: • Storage state and size. • Directory being used. • Maximum number of files.	
Threat Hunting settings: • Whether TAA rules are used to scan chains of events. • Version of the data model being used.	
Time zone settings.	
Update settings: • Update server type. • Custom URL of the update server.	The information is stored indefinitely on the Central Node server in the `/data` directory.
System event log	OS log files are stored indefinitely in the `/var/log` directory on the server hosting the Central Node component.
Log with information about the application operation.	The log file is stored indefinitely in the /data directory on the server hosting the Central Node component, if the component is installed on a server. When the Central Node component is installed on a cluster, data is stored on storage servers indefinitely.
File scan queue.	Files are stored on the server hosting the Central Node component in the /data directory if the component is installed on a server. When the Central Node component is installed on a cluster, data is stored on storage servers. The data is retained until the scan is completed.
Files received from computers with the Endpoint Agent component.	Files are stored on the server hosting the Central Node component in the /data directory if the component is installed on a server. When the Central Node component is installed on a cluster, data is stored on storage servers. Data is rotated when disk space becomes full.
Files with YARA and IDS rules (user-defined and from Kaspersky).	Files are stored indefinitely in the /data directory on the server hosting the Central Node component, if the component is installed on a server. When the Central Node component is installed on a cluster, data is stored on storage servers indefinitely.
Files with data about detections sent to external systems.	Files are stored indefinitely on the server hosting the Central Node component in the /data directory if the component is installed on a server. When the Central Node component is installed on a cluster, data is stored on storage servers indefinitely.
Artifacts of the Sandbox component.	Files are stored on the server hosting the Central Node component in the /data directory if the component is installed on the server. When the Central Node component is installed on a cluster, data is stored on storage servers. Data is rotated when disk space becomes full.
Files for which detections were created by the Sandbox component.	Files are stored on the server hosting the Central Node component in the /data directory if the component is installed on the server. When the Central Node component is installed on a cluster, data is stored on storage servers. Data is rotated when disk space becomes full.

Data type	Location and duration of storage
Certificate files used for the authentication of application components.	Files are stored indefinitely in the /data directory on the server hosting the Central Node, PCN, SCN, Sensor component or on the computer with the Endpoint Agent component.
Encryption keys that are transmitted between application components.	Files are stored indefinitely in the /data directory on the server hosting the Central Node, PCN, SCN, Sensor component or on the computer with the Endpoint Agent component.
Copies of mirrored traffic from SPAN ports.	Files are stored in storage mounted on the server with the Sensor component. Data is deleted as disk space becomes full.

Data type	Location and duration of storage
ICAP exclusion filters.	Files are stored indefinitely on the server hosting the Central Node component in the /data directory if the component is installed on the server. When the Central Node component is installed on a cluster, data is stored on storage servers indefinitely.
• Information about network sessions. • Device information. • Telemetry when integrated with the Endpoint Agent component. • Network traffic events. • User account information. • Information about executable files. • Dumps of traffic relevant to registered events. • Dumps of traffic relevant to network sessions.	The data is stored on the Central Node server in the /data/storage/volumes/nta_database directory. Data is rotated as disk space becomes filled.
• User account ID. • User account name. • Domain name of the user. • User account role. • User account status. • Date and time of the last password change for the user account.	Files are stored indefinitely on the server hosting the Central Node component in the /data directory if the component is installed on a server. When the Central Node component is installed on a cluster, data is stored on storage servers indefinitely.
Virtual machine configuration information: • IP address of the server hosting the Sandbox component • List of virtual machines	

Data type	Location and duration of storage
Data on user accounts: • User account ID. • User account name. • Name of the computer on which the user is authorized.	The data is stored on the Central Node server in the /data/storage/volumes/nta_database directory. Data is rotated as disk space becomes filled.
Network session information: • Names of the participants in the network communication. • IP and MAC addresses of the participants of the network communication.	
Information about devices registered in the application: • Device names. • IP and MAC addresses of devices.	
Data saved when integrated with the Endpoint Agent component as part of the NDR functionality: • IP and MAC addresses of the computer with the Endpoint Agent component. • Name of the computer with the Endpoint Agent component. • Name of the user account registered on the computer with the Endpoint Agent component. • The operating system that the computer is running. • User Agent.	
Information about network traffic events: IP and MAC addresses of devices.	
Information about executable files on Endpoint Agent computers connected as part of the NDR functionality: • File name. • Path to the file. • File version. • MD5 and SHA256 hash of the file.	

Data type	Location and duration of storage
Traffic dump data related to logged network sessions and events: • Names of the participants in the network communication. • IP and MAC addresses of the participants of the network communication. • Device names. • IP and MAC addresses of devices. • User account name. • User account ID. • The operating system that the computer is running. • User Agent. • Name of the executable file. • Path to the executable file. • Version of the executable file. • MD5 and SHA256 hash of the executable file.	
Audit log for user activity related to the NDR functionality.	

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 or deployed as a cluster.

Traffic data is recorded and stored in sequentially created files. The application 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 application is restarted

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

- Information related to alerts generated as a result of scanning by the Targeted Attack Analyzer technology
- PCAP files in which:
  - Source or destination IP address matches an IP address from the detection
  - Traffic data belongs to the time period within 15 minutes from the detection 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 application 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. If the Central Node component is installed on the server, information about alerts and files that resulted in an alert are stored on the server hosting the Central Node component in the `/data/var/lib/kaspersky/storage/pgsql/10/data/` directory. When the Central Node component is installed on a cluster, information about alerts and files that resulted in an alert are stored on the storage servers.

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.
- Category of the detected object.
- Name of the detected file.
- Detected URL.
- MD5 and SHA256 hash of the detected file.
- User comments added to the alert information.
- ID of the TAA rule by which the alert was generated.

- IP address and name of the computer on which the alert was generated.
- ID of the computer on which the alert was generated.

When an alert is changed, the following information is stored on the server:

- The user account that modified the alert.
- The user account to which the alert was assigned.
- Date and time of alert modification.

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.
- All service headers of the message (as they appear in the message).

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

- Name of the computer from which the data was sent.
- Name of the computer that received the data.
- The IP address of the computer from which the data was sent.
- The IP address of the computer that received the data.
- The URI of the transferred resource.
- 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:

- Name of the computer from which the data was sent.
- Name of the computer that received the data.
- The IP address of the computer from which the data was sent.
- The IP address of the computer that received the data.
- Transmitted data.
- Data transfer time.
- URL extracted from the file containing the traffic, User Agent, and method.
- File containing the traffic where the alert occurred.

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.
- Name of the detected object.
- MD5 hash of the detected object.

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

- Version of the program databases used to generate the alert.
- Category of the detected object.
- Names of detected objects.
- MD5 hashes of detected objects.
- Information about detected objects.

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 TAA (IOA) rule.
- Name of the IOC file.
- Information about detected objects.

If the alert was generated by Anti-Malware Engine technology, the following information may be stored on the server:

- Versions of databases of Kaspersky Anti Targeted Attack Platform components that were used to generate the alert.
- Category of the detected object.
- List of detected objects.
- MD5 hash of detected objects.
- Additional information about the alert.

Data in events

Events may contain user data. If the Central Node component is installed on the server, information about occurred events is stored on the server with the component in the `/data/var/lib/kaspersky/storage/fastsearch/elasticsearch/data/` directory. When the Central Node component is installed on a cluster, information is stored on storage servers.

Data is rotated as the disk becomes full.

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.
- Unique ID of the computer with Kaspersky Endpoint Agent.
- Name of the user account under which the event occurred.
- Name of the group that the user belongs to.
- Event type.
- Event time.
- Information about the file for which the event was logged: name, path, full name.
- MD5 and SHA256 hash of the file.
- File creation time.
- File modification time.
- File access rights.

- Environment variables of the process.
- Command-line parameters.
- Text of the command entered into the command line.
- 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.
- Network connection protocol.
- HTTP request method.
- HTTP request header.
- Information about Windows registry variables: path to the variable, variable name, variable value.
- Contents of a script or binary file sent for AMSI scanning.
- 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.

Data in reports

Reports may contain user data. If the Central Node component is installed on the server, information about occurred events is stored indefinitely on the server with the component in the `/data/var/lib/kaspersky/storage/pgsql/10/data/` directory. When the Central Node component is installed on a cluster, information is stored on storage servers.

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.
- ID of the user account that generated 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.
- MD5 and SHA256 hash of the file.
- ID of the user who quarantined the object on the computer with Kaspersky Endpoint Agent.
- ID of the user who placed the object in Storage.
- IP address of the computer on which the quarantined object is stored.
- Name of the computer on which the quarantined object is stored.
- Unique ID of the computer on which the quarantined object is stored in Storage.
- ID of the TAA (IOA) rule by which the alert was generated.
- Category of the detected object.
- Results for the object scanned using individual modules and technologies of the program.

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 t
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 b using operating system t
File scan results	• `/var/opt/kaspersky/sandbox/library/` • `/tmp/`	After the Central Node component receives the scan results or until automatic deletion, but no more than 24 hours.	User access is defined b using operating system t
Task settings	• `/var/opt/kaspersky/sandbox/library/` • 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/`. Up to 90 days in the Sandbox component database.	User access to the direc `/var/opt/kaspersky/` is defined by the adminis operating system tools. A password is required f authentication in the da database files is grantec started database proce root privileges. Access is provided only IPSec channel.
Trace files	`/var/log/kaspersky/sandbox/`	Up to 21 days.	User access is defined b using operating system t Only authorized users ca with trace files. Information about actio saved in the application
Settings of the update source	`/var/opt/kaspersky/apt-updater`	Until modified or deleted.	User access is defined b using operating system t
Minimum password length settings	`/var/opt/kaspersky/apt-config-ram-common/validator.conf`	Until modified or deleted.	User access is defined b using operating system t
Virtual machines	`/vm`	Until modified or deleted.	User access is defined b using operating system t
Downloaded images of operating systems and applications in iso format	`/var/opt/kaspersky/sandbox/custom_images/iso`	Until modified or deleted.	User access is defined b using operating system t

Data transmitted between program components

Central Node and Kaspersky Endpoint Agent for Windows

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

If an event occurs on the user's computer, Kaspersky Endpoint Agent for Windows sends the following data to the events database:

1. General information for all events:
    - Event type.
    - Event time.
    - User account for which the event was generated.
    - Name of the host where the event occurred.
    - IP address of the host.
    - Type of the operating system installed on the host.
2. 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.
3. 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.
    - Registry value name.
    - Registry value data.
    - Registry value type.
    - Previous path to the registry key.
    - Previous registry value data.
    - Previous registry value type.

4. 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.

5. 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.

6. Event in the operating system 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.

- 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.

7. Process start event.

- Information about the process file: file name, file path, MD5 or SHA256 hash of the file, file size, creation and modification date, name of the organization that issued the digital certificate of the file, digital signature verification result.

- UniquePID.

- Process start options.

- Process start time.

- Information about the parent process: file path, UniquePID, MD5 or SHA256 hash of the process file, process start options.

8. Process stop event.

- Information about the file of the process: file name, file path, full name of the file, MD5 or SHA256 hash of the file, file size, and process end time.

- UniquePID.

- Process start options.

- Information about the parent process: file path, UniquePID, MD5 or SHA256 hash of the process file, process start options.

9. 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 name.

- Path to DLL.

- DLL full name.
- MD5 or SHA256 hash of the DLL.
- DLL size.
- Date of DLL creation and modification.
- Name of the organization that issued the digital certificate of the DLL.
- DLL digital signature verification result.

10. 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.
11. 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.
12. Event of Kaspersky Endpoint Security for Windows.
    - 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.
- Contents of the script scanned using AMSI.

13. AMSI scan event.

- Contents of the script scanned using AMSI.

Central Node and Kaspersky Endpoint Agent for Linux

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

If an event occurs on the user's computer, Kaspersky Endpoint Agent for Linux sends the following data to the events database:

1. General information for all events:

- Event type.
- Event time.
- User account for which the event was generated.
- Name of the host where the event occurred.
- IP address of the host.
- Type and version of the operating system that is installed on the host.
- Name of the host that was used to remotely log in to the system.
- Name of the user assigned when registering in the system.
- Group to which the user belongs.
- User name that was used to log in to the system.
- Group of the user whose name was used to log in to the system.
- Name of the user who created the file.
- Name of the group whose users can modify or delete the file.

- Permissions that can be used to gain access to the file.
- Inherited privileges of the file.

2. Process start event.

- Information about the file of the process: file name, file path, full name of the file, MD5 or SHA256 hash of the file, and file size.
- UniquePID.
- Command that was used to start the process.
- Process type.
- Environment variables of the process.
- Process start time.
- Process end time.
- Information about the parent process: file path, UniquePID, MD5 or SHA256 hash of the process file, command that was used to start the process.

3. 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.
- File type.
- MD5 and SHA256 hash of the file.
- Date of file creation and modification.
- File size.

4. Event in the operating system log.

- Event time.
- Event type.
- Result of the operation.
- Information about the parent process: file path, UniquePID, MD5 or SHA256 hash of the process file, command that was used to start the process.

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.
- List of data excluded from the scan.
- 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.
- About the license.
- List of computers with Kaspersky Endpoint Agent.
- Objects placed in Storage.

- Objects quarantined on computers with Kaspersky Endpoint Agent.
- Files attached to alerts.
- IOC and YARA files.

Data contained in application trace files

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 application installed may be granted access to the personal data of other users.

Trace files can include any personal data of the user or confidential data of your organization. Files are stored in the `/var/log/kaspersky` directory indefinitely.

Data of Kaspersky Endpoint Agent for Windows

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

Files prepared by Kaspersky Endpoint Agent for Windows to be sent for scanning to program servers are stored on computers with Kaspersky Endpoint Agent for Windows 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 data from computers with Kaspersky Endpoint Agent for Windows to the server with the Central Node component cannot be disabled.

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

Data received from Kaspersky Endpoint Agent for Windows 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 for Windows to the server with the Central Node component are stored on computers hosting Kaspersky Endpoint Agent for Windows in plain unencrypted form in the same directory that is used as the default directory for storing files on each computer with Kaspersky Endpoint Agent before they are sent.

Files from computers with Kaspersky Endpoint Agent for Windows are only sent to the server with the Central Node component over a secure SSL connection.

Files that have been encrypted on computers with Kaspersky Endpoint Agent for Windows 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 for Windows 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 use the data listed above to ensure the security of computers with Kaspersky Endpoint Agent for Windows as well as Kaspersky Anti Targeted Attack Platform servers. The administrator of Kaspersky Anti Targeted Attack Platform is responsible for access to this information.

This section contains the following information about user data that is stored on computers with Kaspersky Endpoint Agent for Windows:

- 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 program 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. The Kaspersky Endpoint Agent application does not manage access permissions to this folder or 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.

This data can be automatically sent to Kaspersky Security Center.

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.
- Objects blocked in accordance with prevention rules.
- Results of **Delete file** tasks.
- Results of **Kill process** tasks.
- Results of **Run program** tasks.
- Results of **Get file** tasks.
- The active license of Kaspersky Endpoint Detection and Response Optimum.
- Program activation status.

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

Data in Kaspersky Endpoint Agent for Windows 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 program is uninstalled.

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

1. In the synchronization requests:
    - Unique ID of Kaspersky Endpoint Agent.
    - Base part of the server web address.
    - Device name.
    - IP address of the device.
    - MAC address of the device.
    - 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 program settings and task settings.
    - Task statuses in Kaspersky Endpoint Agent: IDs of running tasks, execution statuses, execution error codes.
    - Statuses of Kaspersky Endpoint Agent settings: type of applied settings, version of settings, status of applying the settings, error codes of applying the settings.
2. In requests for obtaining files from the server:
    - Unique IDs of files.
    - Unique ID of Kaspersky Endpoint Agent.
    - Unique IDs of tasks.
    - Base part of the web address of the Central Node server.
    - IP address of the node.

3. In the reports on task execution results:

- IP address of the node.
- Details of objects detected during IOC or YARA scan.
- Flags of the additional actions performed by Kaspersky Endpoint Agent after completion of tasks (for example, `"deleteFileAfterReboot": false`).
- Task execution errors and return codes.
- Task completion statuses.
- Task completion time.
- Versions of settings used for task execution.
- Details of objects submitted to the server, quarantined objects, and objects restored from Quarantine: paths to objects, MD5 and SHA256 hashes of objects, IDs of quarantined objects.
- Details of processes started or stopped on the Kaspersky Endpoint Agent device following the server request: PID and UniquePID, error code, MD5 and SHA256 hashes of objects.
- Information about services started or stopped on the device following the server request (name of the service, run type, error code, MD5 and SHA256 hashes of service file images).
- Details of objects for which a memory dump was created for YARA scanning (paths, dump file ID).
- 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.
  - MD5 hash of the object.
  - SHA256 hash of the object.
- Data on files:
  - Path to the file.
  - File name.

- File size.
- File attributes.
- File creation date and time.
- Date and time of the last modification of the file.
- File description.
- Company name.
- MD5 hash of the object.
- SHA256 hash of the object.
- Registry key (for autorun points).

- Data indicated in errors receiving information about objects:
  - Full name of the object whose processing resulted in the error.
  - Error code.

1. Telemetry data:
   - IP address of the node.
   - 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 that must be used to run tasks.
   - Versions of settings.
   - IDs of quarantined objects.
   - Paths to objects.
   - MD5 and SHA256 hashes of objects.

- Command line to start the process together with the arguments.
- Flags of additional actions performed by Kaspersky Endpoint Agent after completion of the task.
- IOC file identifiers that must be retrieved from the server.
- IOC files.
- Names of services.
- Run type of services.
- Folders for which you need to obtain results of the **Get forensics** task.
- Masks of the names and extensions of objects for the **Get forensics** 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 disabling of isolation.

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.
- Full paths to objects.
- MD5 and SHA256 hashes of objects.
- Identifiers of entries in the 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 for Windows

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 KATA Central Node component.
- Data processed during integration with Kaspersky Industrial CyberSecurity for Networks.

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.

This data can be automatically sent to Kaspersky Security Center.

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 program 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 KATA 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 KATA Central Node component:
    - Updatable telemetry filtering schemes.
    - Telemetry event packet queue.
    - Cache of IOC file identifiers received from the KATA Central Node component.
    - Objects to be passed to the server as part of the **Get file** task.
    - Reports on the **Get forensics** task results.

Kaspersky Endpoint Agent locally stores the following data when integrated with the Kaspersky Industrial CyberSecurity for Networks server:

1. Processed files and data entered by the user during configuration of Kaspersky Endpoint Agent settings:
    - 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 for integration with Kaspersky Industrial CyberSecurity for Networks.
- License data.

2. Data required for integration with Kaspersky Industrial CyberSecurity for Networks.
   - Updatable telemetry filtering schemes.
   - Telemetry event packet queue.

Data contained in Kaspersky Endpoint Agent for Windows trace files and dumps

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

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

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

Do not use Kaspersky Endpoint Agent for Windows 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 for Windows 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 for Windows on the host.
- Information about objects processed by Kaspersky Endpoint Agent for Windows.
- Errors occurring during the operation of Kaspersky Endpoint Agent for Windows.
- 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 for Windows.
- 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 for Windows.
- 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 for Windows.
- Names of files on computers with Kaspersky Endpoint Agent for Windows.
- Full names of folders on computers with Kaspersky Endpoint Agent for Windows.
- 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 the KSN Statement was 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 program 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. The Kaspersky Endpoint Agent application does not manage access permissions to this folder or 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. The Kaspersky Endpoint Agent application does not manage access permissions to this folder or 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 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. The Kaspersky Endpoint Agent application does not manage access permissions to this folder or 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. The Kaspersky Endpoint Agent application does not manage access permissions to this folder or any files in it. It is the system administrator who determines access permissions.

Data of Kaspersky Endpoint Agent for Linux

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

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

Transmission of data from computers with Kaspersky Endpoint Agent for Linux to the server with the Central Node component cannot be disabled.

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

Data received from Kaspersky Endpoint Agent for Linux 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 Endpoint Agent for Linux to the server with the Central Node component are stored on computers hosting Endpoint Agent for Linux in plain unencrypted form in the same directory that is used as the default directory for storing files on each computer with Kaspersky Endpoint Agent before they are sent.

Files from computers with Kaspersky Endpoint Agent for Linux are only sent to the server with the Central Node component via a secure SSL connection.

The Kaspersky Anti Targeted Attack Platform administrator must take steps to ensure the security of computers with Kaspersky Endpoint Agent for Linux 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 Endpoint Agent for Linux:

- 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 program is uninstalled.

Data in Kaspersky Endpoint Agent for Linux 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 for Linux installed:

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

1. In the synchronization requests:
    - Unique ID of Kaspersky Endpoint Agent for Linux.
    - Device name.
    - Local time on the device.
    - Name and version of the operating system that is installed on the device.
    - Version of Kaspersky Endpoint Agent for Linux.
    - Versions of program settings and task settings.
    - Task statuses in Kaspersky Endpoint Agent for Linux: identifiers of running tasks, execution statuses, execution error codes.
2. Data on running processes:
    - Information about the executable file of the process. For the scope of data about the file, see below.
    - Process autorun settings.
    - Values of environment variables.
    - Process ID.
    - Parent process ID.
    - Logon session code.
    - Logon session name.

- IDs of users and groups that started the process.
- Date and time when the process started.
- Information about stopped processes:
  - Process ID.
  - Date and time when the process was stopped.
- Data on files:
  - Path to the file.
  - File name.
  - File size.
  - File attributes.
  - File creation date and time.
  - Date and time of the last modification of the file.
  - Names and unique IDs of the user and group that own the file.
  - Access rights of the file.
  - Unique identifier of the file.
- Information about file modifications:
  - Unique identifier of the file.
  - Type of operation performed on the file (writing, reading, attribute modification, renaming, deletion).
- Information about the logon session:
  - Date and time when the logon session began.
  - Type of the session.
  - Name of the user that initiated the session.
  - Type of the user that initiated the session.
  - Remote computer IP address.
- Information about alerts on the computer with Kaspersky Endpoint Agent for Linux and Kaspersky Endpoint Security for Linux.
  - Type of detected object.
  - Name of the object and full path to the object.

- Name of the alert.
- MD5 hash of the object.
- URL from which the object was downloaded.
- Remote computer IP address.
- IP address of the local computer.
- Alert processing result.

Before it is sent, data is stored in the /var/opt/kaspersky/epagent/data/cache/queue directory in plain unencrypted form. By default, only users with root permissions have access to the files.

3. Settings of tasks received by Kaspersky Endpoint Agent for Linux from the Central Node:

- Task types.
- Task schedule settings.
- Names and passwords of the accounts under which the tasks can be run.
- Versions of settings.
- Paths to objects.
- MD5 and SHA256 hashes of objects.
- Command line to start the process together with the arguments.
- Information about the individual task is stored on the device until Kaspersky Endpoint Agent receives a deletion request from the Central Node or until Kaspersky Endpoint Agent itself is removed from the device.

Task data is stored in the /var/opt/kaspersky/epagent/tasks directory in plain unencrypted form. By default, only users with root permissions have access to the files.

4. In the reports on task execution results sent by Kaspersky Endpoint Agent for Linux to the Central Node:

- Task execution errors and return codes.
- Task completion statuses.
- Task completion time.
- Versions of settings used for task execution.
- Information about objects sent to the server (paths to objects, MD5 and SHA256 hashes of objects).
- Files requested by the server.

- Content of the process standard output.
- Content of the process standard error stream.
- Kaspersky Endpoint Agent for Linux sends task execution result reports to the Central Node.

Task execution result data is stored in the /var/opt/kaspersky/epagent/tasks directory in plain unencrypted form. By default, only users with root permissions have access to the files.

Information with the task execution report is deleted after the information is sent to the Central Node.

Service data of Kaspersky Endpoint Agent for Linux

Service data of Kaspersky Endpoint Agent for Linux includes data that is stored in configuration files as a result of an administrator configuring settings locally or using the Kaspersky Security Center plug-in.

Service data is stored in the /var/opt/kaspersky/epagent/settings and /var/opt/kaspersky/epagent/policy directories. The data is stored until Kaspersky Endpoint Agent for Linux is uninstalled.

This data can be automatically sent to Kaspersky Security Center.

By default, only users with root permissions have access to the files.

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

Kaspersky Endpoint Agent for Linux stores the following data:

- Address of the Central Node server.
- Public key of the server certificate for integration with the Central Node.
- Container with the client certificate for integration with the Central Node.
- Authorization credentials for the proxy server.
- Addresses of custom update sources.
- Configuring the frequency of synchronization and sending telemetry to the Central Node server.

Data contained in Kaspersky Endpoint Agent for Linux trace files and dumps

Data contained in trace files

Users are responsible for the security of data stored on their computers, in particular for monitoring and restricting access to the data before it is sent to Kaspersky.

Trace files are stored on the computer during the entire period the program is used and are permanently deleted when the program is removed.

By default, trace files are saved in the /var/log/kaspersky/epagent/ directory. You can view data in trace files. Accessing the default trace file directory requires root permissions.

All trace files contain the following general data:

- Time when the event occurred.
- Number of the thread of execution.
- Program component that initiated the event.
- Event importance level (information, warning, critical, error).
- Description of the event that occurred in connection with a program component running a command, and the result of the command.

In addition to general information, trace files can contain the following data:

- Kaspersky Endpoint Agent component statuses and their working data
- Information about all operating system objects and events including user activity information
- Data contained in operating system objects (for example, contents of files that can include personal data of users)
- Network traffic data (for example, contents of website forms that can include bank card data or other confidential data)
- Data received from Kaspersky servers (for example, version of the program databases)

Trace data is recorded to the lena2021-01-18T052236.log file. When the file size reaches 10 MB, the file is saved in the /var/log/kaspersky/epagent/ directory. A new file with a timestamp is created to record current data. Up to 10 files with trace data can be stored in the directory. When the size of the last created file reaches 10 MB, the oldest file is deleted.

Trace files of other programs are stored on the computer until the program is removed.

Data contained in dump files

Stored dump files can contain personal data. To monitor and restrict access to data, you must take steps to ensure the security of dump files.

Dump files are generated automatically whenever the program crashes, and are stored on the computer during the entire period when the program is used. Dump files are permanently deleted when the program is removed.

Dump files are stored in the /var/opt/kaspersky/epagent/dumps/ directory.

A dump file contains the entire memory dump of Kaspersky Endpoint Agent for Linux processes for the moment when the dump file is created. The dump file can also contain personal data.

Accessing dump files requires root permissions.

Application 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 application.

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

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 application distribution kit.
- In the application web interface, in the **Settings** section, **License** subsection, by clicking the **License Agreement** button.
- In the web interface of the Sandbox component, in the ⓘ menu, by clicking the **End User License Agreement** link.

By confirming that you agree with the End User License Agreement when installing the application, 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 application installation and must not use the application.

About the license

A license is a limited-time right to use Kaspersky Anti Targeted Attack Platform granted under the terms and conditions of the End User License Agreement (EULA).

The list of available functionality and the period for which you can use the application depend on the license under which you are using the application.

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.

The update functionality (including anti-virus signature updates and code base updates), as well as the KSN functionality may be unavailable in the territory of the USA.

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

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

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

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

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

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

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

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

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

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

To view the text of the End User License Agreement in the web interface of the Sandbox server:

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 application.
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 **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 **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 **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**, **Custom 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 program 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**, **Custom rules**, **Storage**, and **Endpoint Agents** have limited functionality.

Architecture of the application

The application includes the following main components:

- *Sensor*. Receives and scans data, can also be used as a proxy server during data exchange between Endpoint Agent and Central Node.
- *Central Node*. Receives and scans data, analyzes the behavior of objects, and publishes analysis results in the web interface of the application.
- *Sandbox*. Starts virtual images of operating systems. Starts files in these operating systems and tracks the behavior of files in each operating system to detect malicious activity and signs of targeted attacks to the corporate IT infrastructure.
- *Endpoint 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 programs 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 also be used as a proxy server for outgoing connections from Kaspersky Endpoint Agent.

If KSMG or KLMS is being used as a Sensor component, scan exclusion 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 component can be deployed on one server or as a fault-tolerant cluster that consists of 2 roles: storage servers and processing servers.

Fault tolerance is achieved through duplication of data between the storage servers and the redundancy of computing resources: if one server fails, its functions are performed by another server with the same role. Meanwhile, the Kaspersky Anti Targeted Attack Platform continues to work.

The following program modules, kernels and technologies run on each server or cluster with 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.
- CentOS 7.8.

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

The component is represented by Kaspersky Endpoint Agent for Windows and Kaspersky Endpoint Agent for Linux programs. The programs are 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 programs continually monitor processes, active network connections, and files being modified, and send this monitoring data to the Central Node server.

Computers where the programs are installed must satisfy hardware and software requirements of Kaspersky Endpoint Agent for Windows and Kaspersky Endpoint Agent for Linux.

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 key 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.

Sensor, Central Node and Sandbox interoperate 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).

    IDS technology can recognize and detect network activity in 80 protocols, particularly in 53 application layer protocols of the TCP/IP model, detecting suspicious traffic and network attacks. Supported protocols include TCP, UDP, FTP, TFTP, SSH, SMTP, SMB, CIF, SSL, HTTP, HTTP/2, HTTPS, TLS, ICMPv4, ICMPv6, IPv4, IPv6, IRC, LDAP, NFS, DNS, RDP, DCERPC, MS-RPC, WebSocket, Citrix and others.
  - 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 component is represented by Kaspersky Endpoint Agent for Windows and Kaspersky Endpoint Agent for Linux programs.

- Sandbox.

  Optional component.

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

Kaspersky Endpoint Agent and Central Node components interoperate as follows:

- Kaspersky Endpoint Agent for Windows and Kaspersky Endpoint Agent for Linux are installed on individual computers in the corporate IT infrastructure and continuously monitor processes, open network connections and files being modified. The monitoring data are sent to the server with the Central Node component. Events are generated based on these data.

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

  - **Process started**
  - **Module loaded**
  - **Connection to remote host**
  - **Prevention rule**
  - **Document blocked**

- **File changed**
- **System event log**
- **Registry modified**
- **Port listened**
- **Driver loaded**
- **Process: interpreted file run**
- **Process: console interactive input**

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

- **Process started**
- **File changed**
- **System event log**

The programs can integrate with workstation protection programs (Endpoint Protection Platform (hereinafter also "EPP")).

Kaspersky Endpoint Agent for Windows can integrate with the following EPP programs:

- Kaspersky Endpoint Security for Windows.
- Kaspersky Security for Windows Server.
- Kaspersky Security for Virtualization Light Agent for Windows.

Kaspersky Endpoint Agent for Linux can integrate with Kaspersky Endpoint Security for Linux.

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.

EPP programs, Kaspersky Endpoint Agent, and Central Node components interoperate as follows:

- EPP programs send information about detected threats and results of threat processing to Kaspersky Endpoint Agent.

  Kaspersky Endpoint Security for Windows can also supply Kaspersky Endpoint Agent for Windows with information about third-party applications with Antimalware Scan Interface support (hereinafter also referred to as "AMSI") sending objects (for example, PowerShell scripts) to Kaspersky Endpoint Security for Windows for additional scanning.

- 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.

  EPP program data processing generates **Scan: detect**, **Scan: detect processing result**, **AMSI scan** events (when Kaspersky Endpoint Agent for Windows is integrated with Kaspersky Endpoint Security for Windows).

  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. If you have the Sandbox component, you can also automatically send files from Kaspersky Endpoint Agent hosts to be scanned by the Sandbox component in accordance with Kaspersky TAA (IOA) rules.

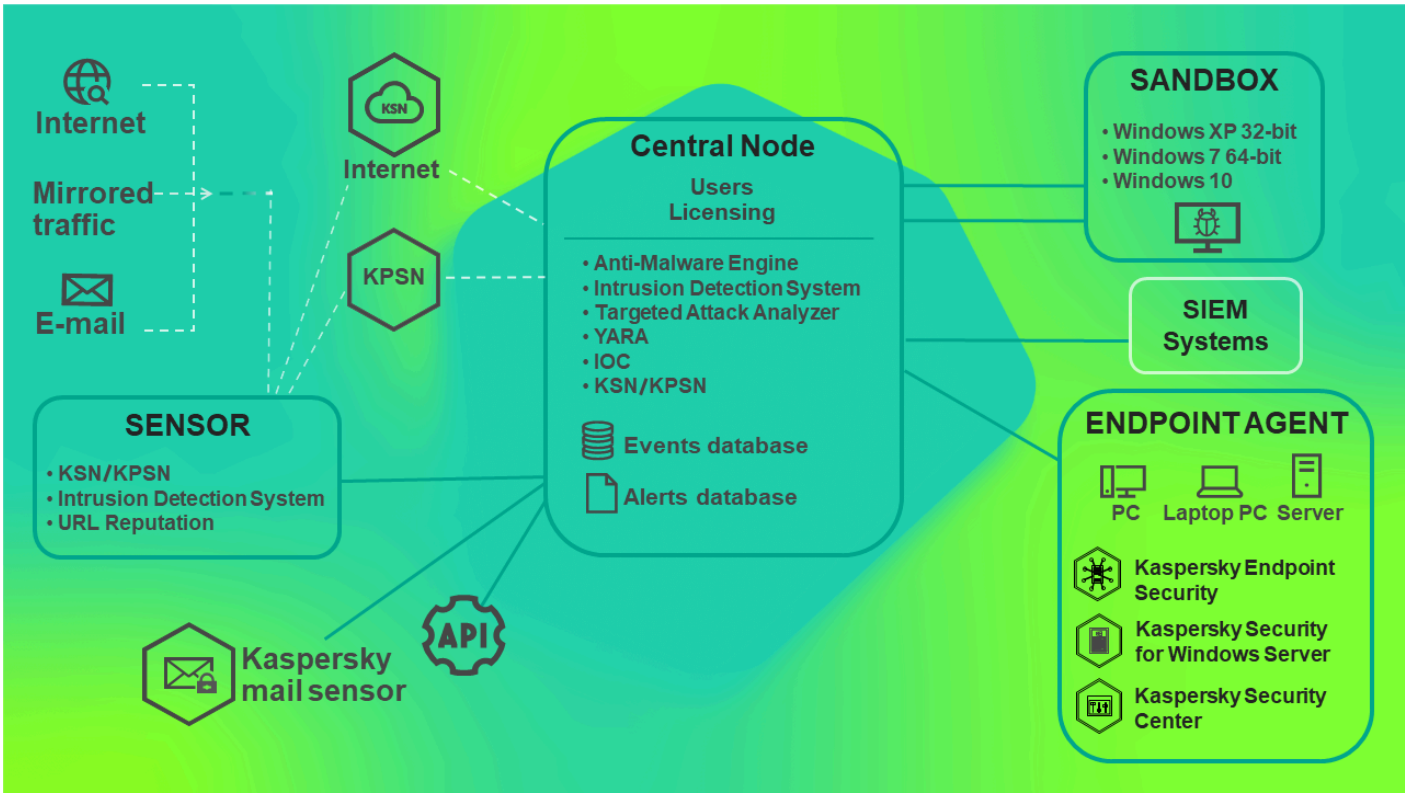
When the Central Node server is integrated with Kaspersky Endpoint Agent for Windows, you can do the following to react to detected threats:

- Manage files and programs by running the following tasks on Kaspersky Endpoint Agent hosts: **Kill process**, **Get forensics**, **Start YARA scan**, **Run program**, **Get file**, **Delete file**, **Quarantine file**, **Restore file from quarantine**, **Service management**, **Get disk image**, **Get memory dump**.
- Configure policies for preventing the running of files and processes on selected Kaspersky Endpoint Agent hosts.
- Isolate individual 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.

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

- Manage files and programs by running tasks: **Get file**, **Run program**.
- Work with TAA (IOA) rules to classify and analyze events.

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

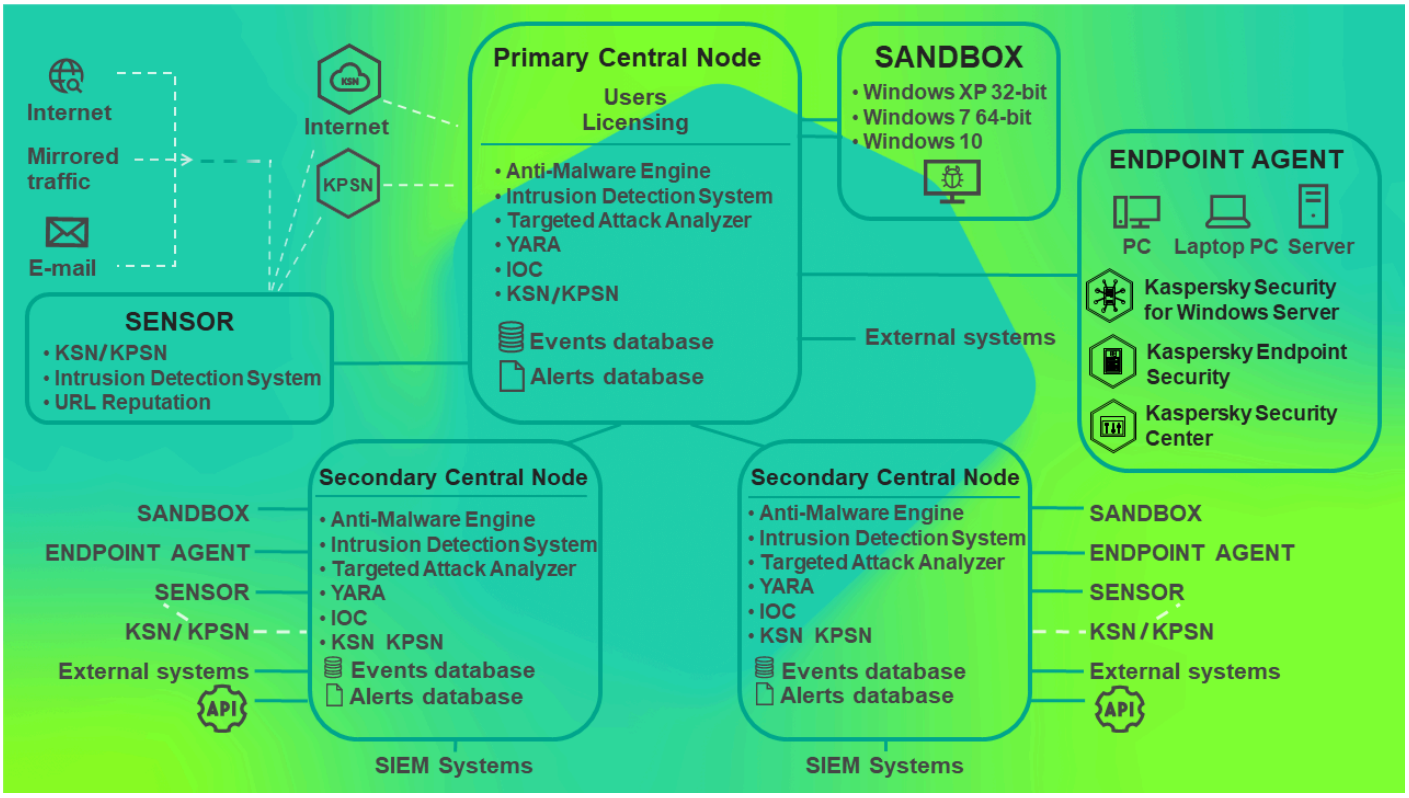


Principle of operation of Kaspersky Anti Targeted Attack Platform

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 primary control server known as the Primary Central Node (PCN) and secondary 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

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 primary control server known as the *Primary Central Node (PCN)* and secondary servers known as *Secondary Central Nodes (SCN)*. Interaction of servers requires connecting SCN to PCN.

If you have deployed the Central Node component as a cluster, the entire cluster takes on the role of a PCN or SCN.

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:

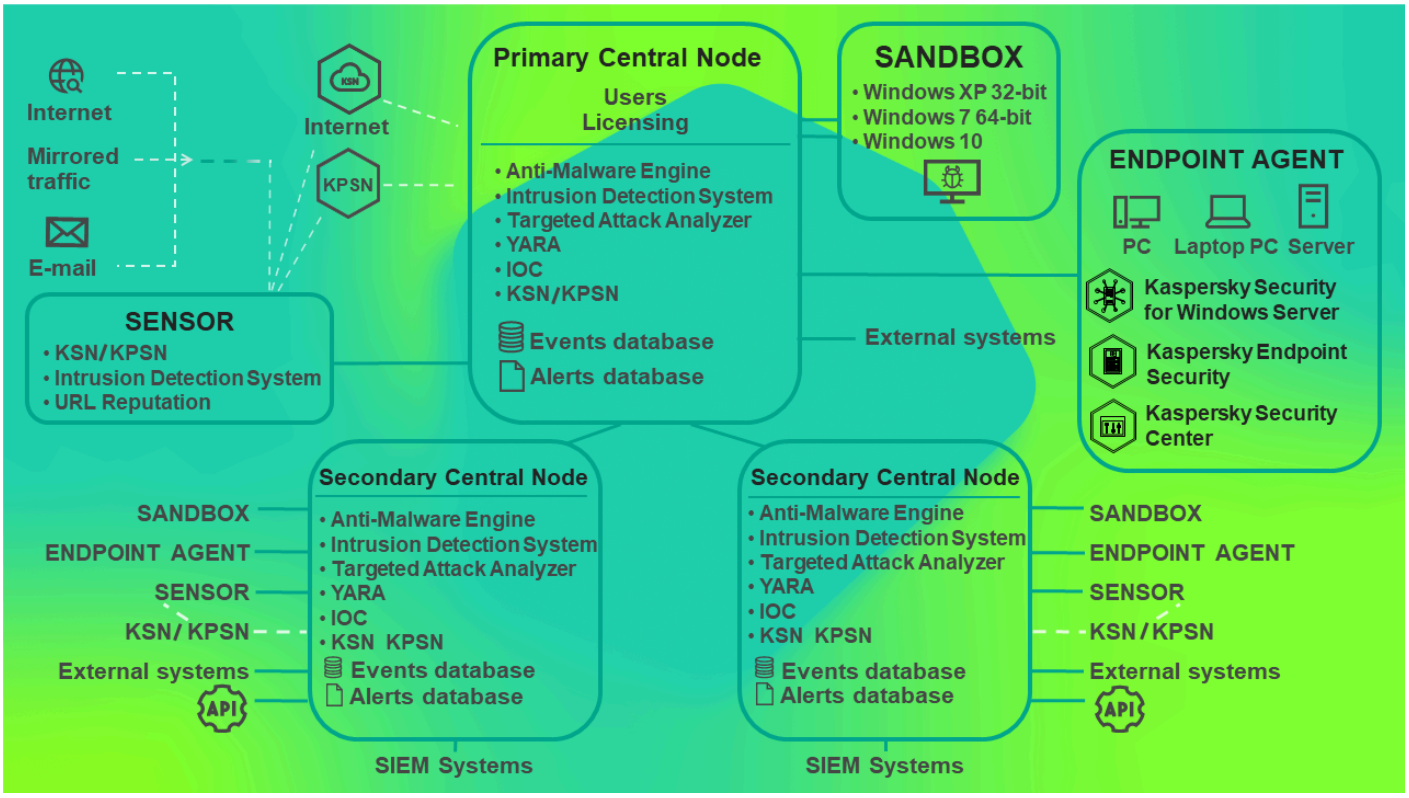
- Users.
- Alerts.
- Threat Hunting.
- Tasks.
- Prevention.
- Custom rules.
- Storage.
- Endpoint Agents, including network isolation of hosts.
- Reports.

If you are supporting multiple organizations or branch offices of the same organization, you can use the program in multitenancy mode.

Multitenancy mode lets you use the solution to protect the infrastructure of multiple organizations or branch offices of the same organization (hereinafter also referred to as "tenants") simultaneously. You can install Kaspersky Anti Targeted Attack Platform on one or more Central Node for each tenant. Each tenant can manage the program independently from other tenants. The service provider can manage the data of multiple tenants.

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 log 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 the distributed solution and multitenancy mode in the following cases:

- To protect more than 10,000 hosts of a tenant
- For centralized management of the program in different departments of the tenant
- For centralized management of the program on servers of multiple tenants

When the program switches to the distributed solution and multitenancy mode, all previously added license keys are deleted from servers with the SCN role. Each connected SCN receives a key from the PCN. If full functionality of the program is used for the PCN (KATA and KEDR key), and partial functionality is used for the SCN (only KATA key or only KEDR key), the SCN server load limit may be exceeded because of the increased volume of data. If partial program functionality is used for the PCN (only KATA key or only KEDR key), and full functionality is used for the SCN (KATA and KEDR key), the program functionality is partially unavailable.

License keys can be managed only on the PCN.

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

- 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 5.0.

Before you switch servers with Central Node components installed to distributed solution mode, you should 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 solution and multitenancy mode transition scenario

Switching the program to the distributed solution 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 the distributed solution and multitenancy mode

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

Modifications of program settings for the distributed solution 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. After that, the SCN requests a list of users from the PCN and uses that list to create local users with the same parameters: • Name • Password • Role • Status 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 must be displayed in the widget. 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. 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. Settings of tasks created on the PCN cannot be changed.

Functional area	PCN	SCN
Reports	Templates and reports created before the switch to distributed solution mode are preserved. A **Servers** column is added to the report table, containing information about the relevant SCN for the alert. After switching to distributed solution mode, only reports created on a PCN are displayed.	Templates and reports created before the switch to distributed solution mode are preserved. 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. After switching to distributed solution mode, only reports created on an SCN are displayed.
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. Policies created on SCNs are also displayed in the policy list. Settings of these policies cannot be changed on the PCN.	Policies created on the PCN are displayed, as well as policies created on this SCN. Settings of policies created on the PCN cannot be changed.
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. 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 exclusions	No changes.	No changes.
VIP status	No changes.	No changes.
Notification rules	No changes.	No changes.
Integration with mail sensors	No changes.	No changes.
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 tenant is displayed.	No changes.
Custom rules - TAA	IOC files added on the Central Node server before it was assigned the PCN role are applied to the PCN. 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. To back up the program on a PCN, disconnect all SCNs from the PCN.	Backup of the program on an SCN is not available. To back up the program on an SCN, disconnect that server from the PCN by switching it to standalone server 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 the server:

1. Log in to the program web interface with the administrator account.

   You need to log in to the web interface of the server to which you want to assign the PCN role.

2. Select the **Operation mode** section.

3. Click **Distributed solution**.

4. In the **Server role** drop-down list, select **Primary Central Node**.

5. In the **Tenant name** field, enter the name of the tenant 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 tenant.

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

- **Current mode** – Distributed solution.
- **Server role** – Primary Central Node.
- **Certificate fingerprint** – the fingerprint of the server's certificate required for authentication when establishing connection with an SCN.
- **Tenants** – information about tenants to which this server and connected SCN servers belong:
  - **IP** – Primary Central Node for this server and IP addresses of SCN servers (after they connect).
  - **Server** – name of this server and names of SCN servers (after they connect).

    This name is not related to name of the host where the program is installed. You can change it.
  - **Certificate fingerprint** – blank value for this server and certificate fingerprints of SCN servers (after they connect).
  - **Status** – connection state of SCN servers (after they connect) and the number of servers connected to tenants.
- The **Servers pending authorization** table contains information about connected SCN.

Assigning the SCN role to a server

To assign the SCN role to the server:

1. Log in to the program web interface with the administrator account.

   You need to log in to the web interface of the server to which you want to assign the SCN role.
2. Select the **Operation mode** section in the window of the program web interface.
3. Click **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 **Operation mode** 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 is assigned to the tenant specified by the PCN administrator.

Processing SCN to PCN connection requests

To process a SCN to PCN connection request:

1. Log in to the program web interface with the administrator account.

   You need to log in to the web interface of the PCN server that you want to use to process connection requests from other servers.

2. Select the **Operation mode** section in the window of the program web interface.

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

3. Contact the SCN administrator who sent the connection request and verify the certificate fingerprint in the **Servers pending authorization** table. It must match the fingerprint displayed on the SCN in the **Certificate fingerprint from request** field of the **Operation mode** section.

4. If certificate fingerprints on the PCN and the SCN match, do one of the following:

   - If you want to reject the connection request from the SCN, click **Reject**.
   - If you want to accept the connection request from the SCN:

     1. Click **Accept**.

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

     2. In the **Tenant** list, select the tenant to which you want to assign this SCN server. The list includes previously added tenants.

     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 tenants, 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 PCN and SCN servers in multitenancy mode:

1. Log in to the program web interface with the administrator account.

   You need to log in to the web interface of the PCN server.

2. Select the **Operation mode** section in the window of the program web interface.

The workspace displays the following information about servers:

- **Current mode** – Distributed solution.
- **Server role** – Primary Central Node.
- **Certificate fingerprint** – certificate fingerprint of the PCN server.
- **Tenants** – information about tenants to which the server belongs, as well as all SCN servers connected to the PCN.
  - **IP** – Primary Central Node for the PCN server and IP addresses of SCN servers connected to the PCN.
  - **Server** – name of the server and names of SCN servers that connect to the PCN.

    This name is not related to name of the host where the program is installed. You can change it.
  - **Certificate fingerprint** – blank value for the PCN server and certificate fingerprints of SCN servers waiting to connect to the PCN.
  - **Status** – connection status of SCN servers and the number of servers connected to the tenant.
- The **Servers pending authorization** table contains the following information:
  - **IP** – IP address or domain name of the SCN server.
  - **Server** – name of the SCN server that is displayed in the program web interface.

    This name is not related to name of the host where the program is installed. You can change it.
  - **Certificate fingerprint** – certificate fingerprint of the SCN server that is sent to the PCN with the connection request.
  - **Status** – status of the SCN to PCN connection.

Adding a tenant to the PCN server

To add a tenant in the PCN server web interface:

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

The tenant is added and is displayed in the list.

Deleting a tenant from the PCN server

To delete a tenant in the PCN server web interface:

1. Log in to the program web interface with the administrator account.
   You must log in to the web interface of the PCN server for which you want to delete a tenant.
2. Select the **Operation mode** section in the window of the program web interface.
3. In the **Tenants** workspace, select the tenant 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 tenant are lost.

5. Click **Yes**.

The tenant is deleted.

Renaming a tenant on the PCN server

To rename a tenant in the web interface of the PCN server:

1. Log in to the program web interface with the administrator account.
   You must log in to the web interface of the PCN server for which you want to rename a tenant.

2. Select the **Operation mode** section in the window of the program web interface.

3. In the **Tenants** list, click next to the tenant that you want to rename.

   This opens a window in which you can rename the tenant.

4. In the **Name** field, enter the new name of the tenant.

5. Click **Save**.

The tenant is renamed.

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 tenant to another, you must 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 tenant.

To disconnect the SCN from the PCN 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 that you want to disconnect the SCN from.

2. Select the **Operation mode** section in the window of the program web interface.

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

4. Click **Disconnect**.

   This opens the action confirmation window.

5. Click **Yes**.

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

To disconnecting the SCN from the PCN through the SCN web interface:

1. Log in to the program web interface with the administrator account.

   Log in to the web interface of the SCN server that you want to disconnect from the PCN.

2. Select the **Operation mode** section in the window of the program web interface.

3. Click **Disconnect**.

   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. Information about changes of the user account that has rights on the disconnected SCN is not sent to the SCN.	User accounts received from the PCN are not deleted. You can create new user accounts again, as well as disable and change passwords for existing user accounts.
Alerts	Alert information on the disconnected SCN is deleted.	Operation history and all alert information is preserved.
Tasks	Tasks created on the disconnected SCN are deleted.	Tasks created on the PCN are deleted. Information about users who created tasks on the SCN is preserved.
Reports	All reports created earlier concerning the disconnected SCN are preserved, as well as the ability to filter the report list by this server.	Templates and reports are not modified.
Prevention	Policies created on the disconnected SCN are deleted.	Policies created on the PCN are deleted. Information about users who created policies on the SCN is preserved.
Storage	All objects related to the disconnected SCN are deleted from Storage.	All objects in the Storage are preserved. The link to the task stops working in information about objects received as part of tasks created on the PCN.
TAA exclusions	No changes.	No changes.
VIP status	No changes.	No changes.
Notification rules	No changes.	No changes.
Integration with mail sensors	No changes.	No changes.
Threat Hunting	After the search query is processed, events related to the disconnected SCN are not displayed.	No changes.
Custom 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.

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 tenant to another, you must 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 tenant.

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 **Operation mode** section in the window of the program web interface.
3. In the server list, select the SCN that you want to delete.
4. Click **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 10,000	From 5000 to 10,000	Over 10,000
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

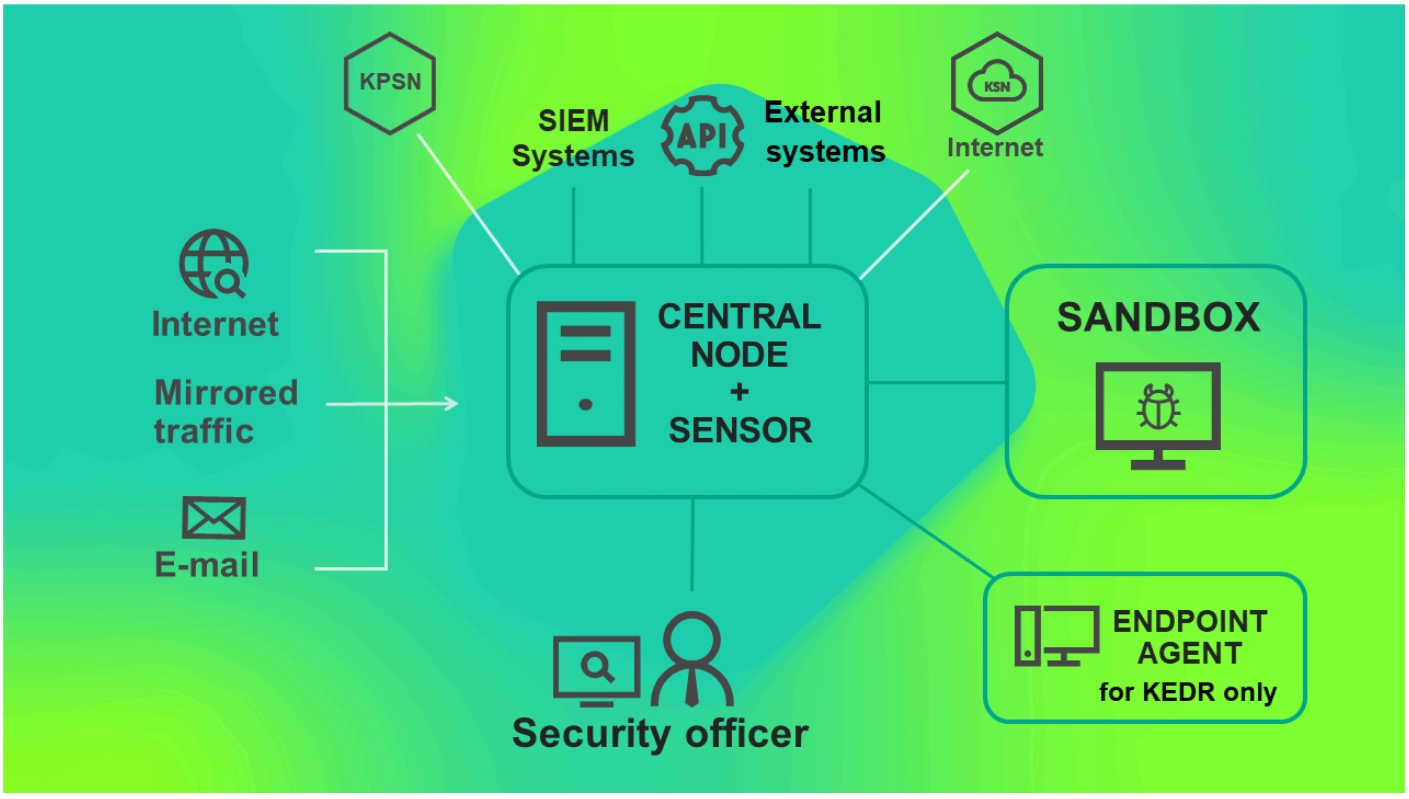
Two-server deployment scenario.

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 using this deployment scenario, the Central Node and Sensor components are installed on the same server or cluster. This server or cluster 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.

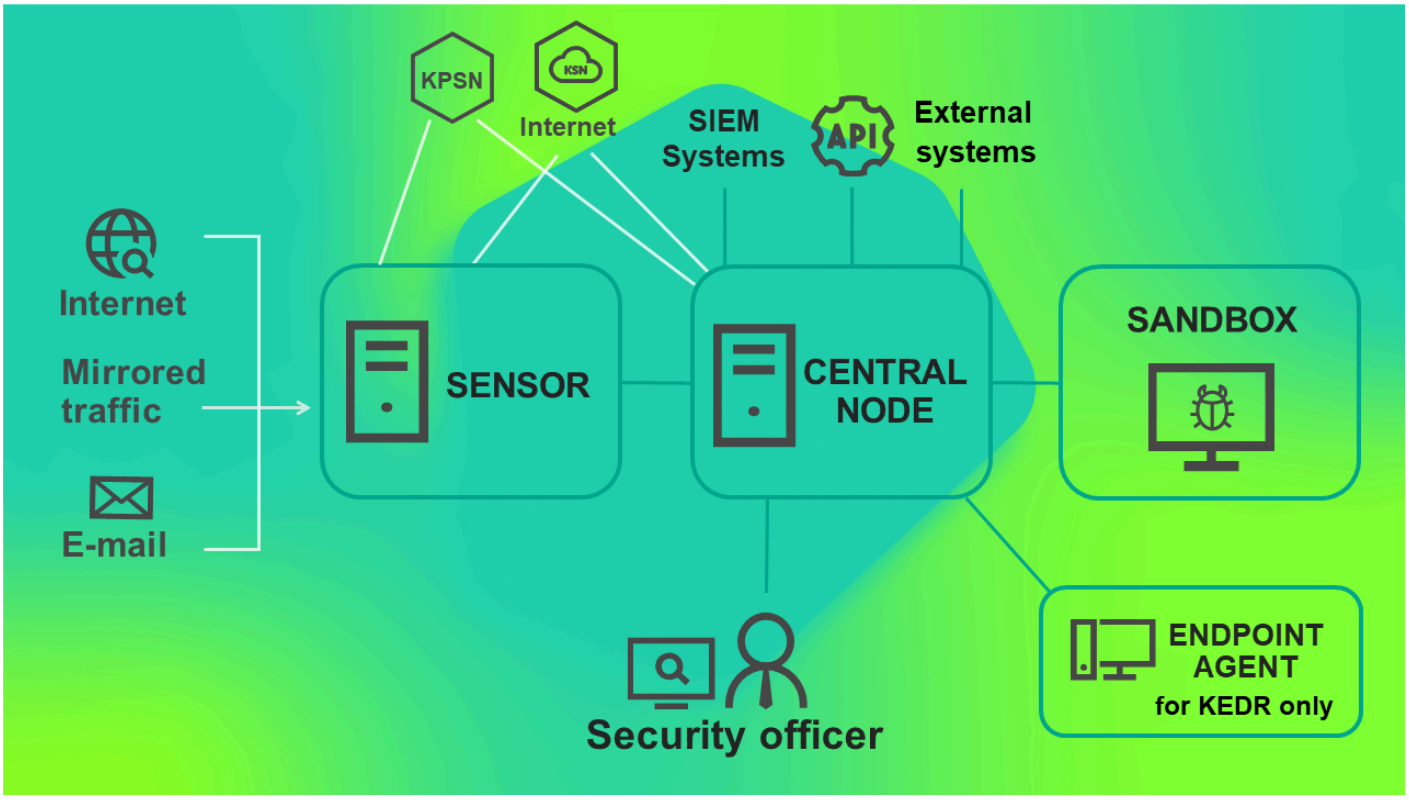
When using KATA and KEDR functionality, you can install the Kaspersky Endpoint Agent program on corporate LAN computers. When using KATA functionality, the Kaspersky Endpoint Agent program is not installed.

When using this deployment scenario, the Sensor, Central Node and Sandbox components are installed on separate servers. The Central Node component can also be deployed as a cluster. The server with the Sensor component receives traffic, performs an initial analysis, extracts files and forwards them to 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 exchanged 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

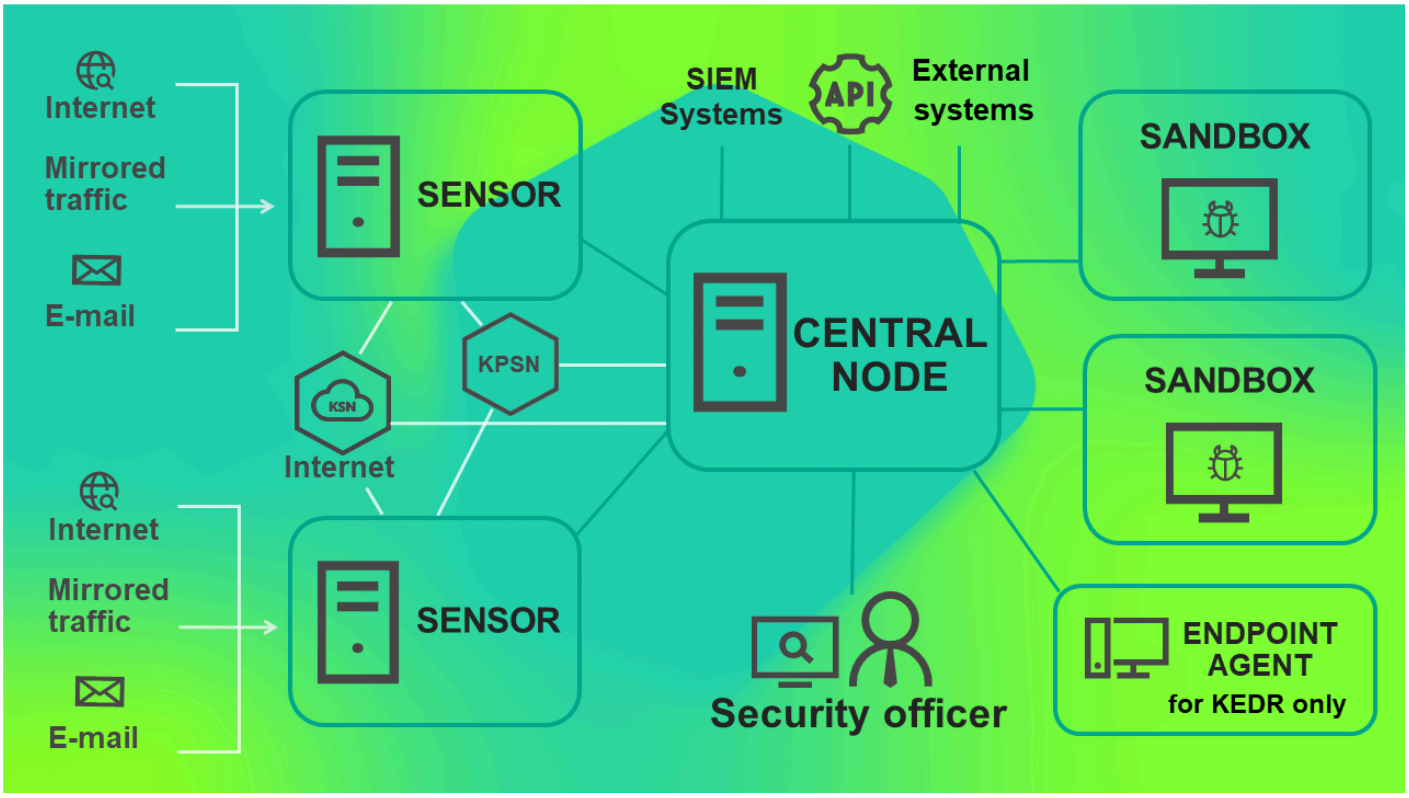
Scenario of deployment on four or more servers.

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.

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.

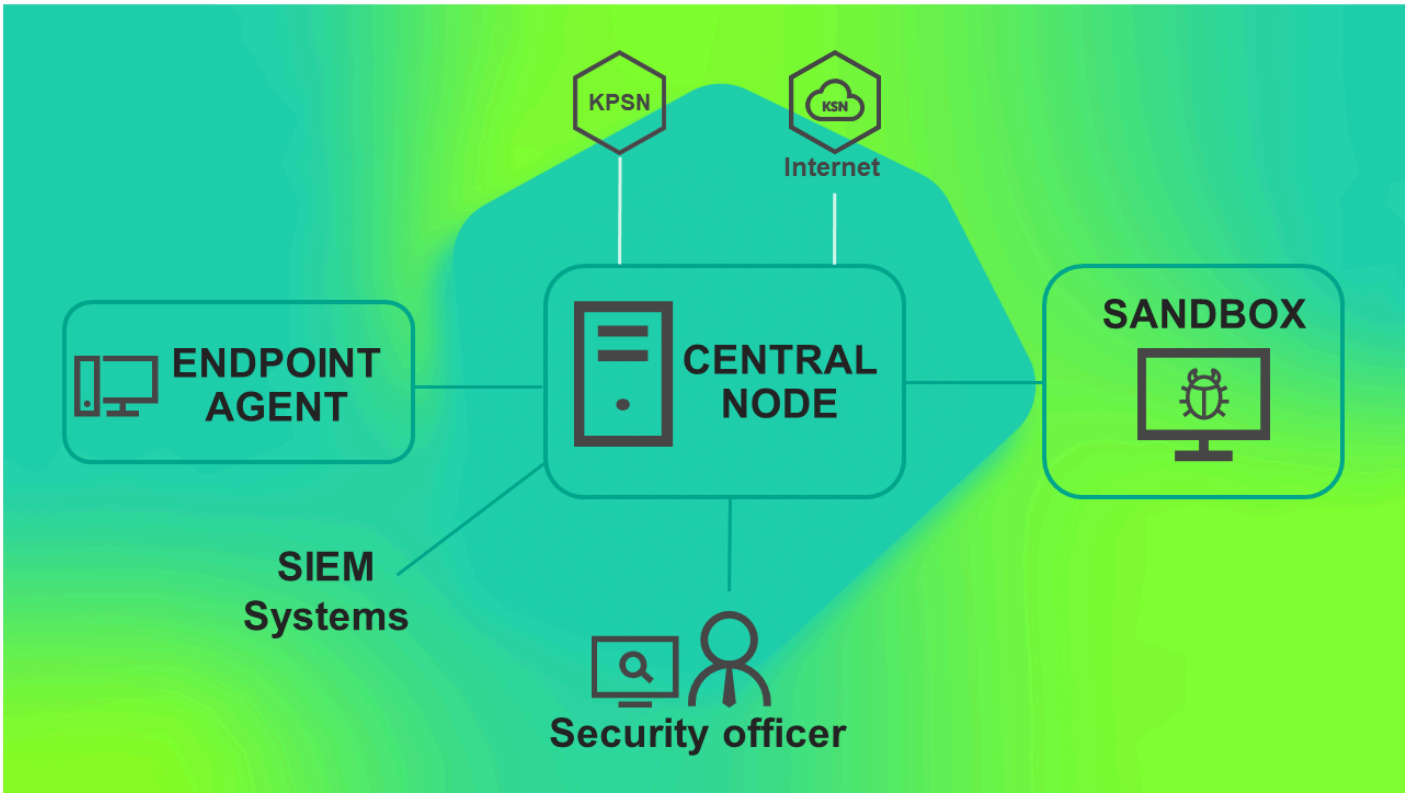


Program operating scenario when deployed on four or more servers

Scenario for deploying KEDR functionality with a Sandbox component.

Using this deployment scenario, you need to install the Central Node component separately from the Sensor component.

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



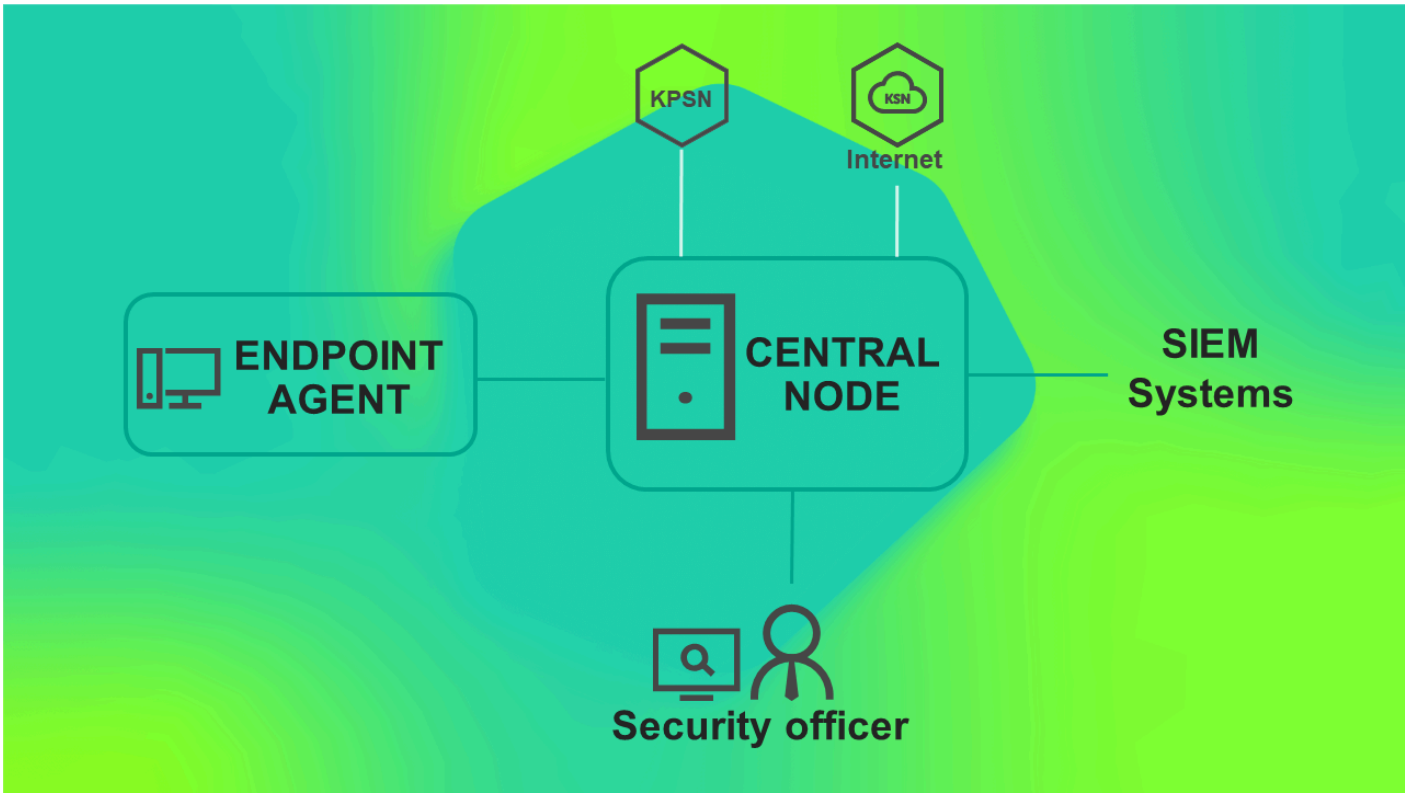
Program operating scenario when deploying KEDR functionality with the Sandbox component

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.

Using this deployment scenario, you need to install the Central Node component separately from 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 application components.

The hardware requirements for 7.1 Central Node servers are different from the hardware requirements of the previous version of the component. We strongly recommend making sure that your server configuration satisfies the requirements listed in the *Calculations for the Central Node component* section.

If necessary, you can use version 7.1.1 or 7.1.2 of the application on hardware designed for version 5.1 of the application.

In this case, the following restrictions apply:

- You can only use the application functionality that is available in version 5.1. If you want to use the functionality of other versions of the application, the hardware of the Central Node servers must satisfy the hardware requirements listed in the Help for those versions.

  List of functionality that is not available in Kaspersky Anti Targeted Attack Platform 5.1

Kaspersky Anti Targeted Attack Platform 6.0

- ICAP integration with feedback.
- Detection of threats in the SMB, NFS, HTTP2 protocols.
- Scanning of mirrored encrypted traffic thanks to integration with the ArtX TLSproxy 1.9.1 application.
- Traffic capture and analysis at speeds up to 10 Gbps.
- Recording, storing and downloading copies of mirrored traffic from SPAN ports.
- Automatic removal of inactive hosts displayed in the Endpoint Agents list on the server with the Central Node component.
- Expanded functionality for hosts that have Kaspersky Endpoint Security for Linux 12 as the Endpoint Agent component.
  - The **Delete file** task.
  - The **Kill process** task.
  - Isolation of individual hosts from the network.
  - Support for files conforming to the OpenIOC open standard for the description of indicators of compromise (IOC files).

Kaspersky Anti Targeted Attack Platform 6.1

- NDR license key.
- Detection of threats in encrypted traffic without decryption using ja3 and ja3s methods and the ability to load custom rules for analyzing encrypted traffic.
- Detection of threats when scanning chains of events using Kaspersky TAA (IOA) rules.
- Viewing screenshots of files being executed by the Sandbox component in the alert card.

Kaspersky Anti Targeted Attack Platform 7.0

- Connecting up to 150 SCN servers to a single PCN server in distributed solution and multitenancy mode.
- Manually sending files for scanning in Sandbox from hosts on which Kaspersky Endpoint Security for Windows and Kaspersky Endpoint Security for Linux are used in the role of the Endpoint Agent component.
- Creating TAA (IOA) rules based on event search conditions from a YAML file with a Sigma rule.

- Expanded list of fields available for event search in source code mode in the **Threat Hunting** section.
- Expanded functionality for the Endpoint Agent represented by Kaspersky Endpoint Security for Windows 12.7:
  - Events: **Code injection**, **Named pipe**, **WMI**, **LDAP**, **DNS**, **Process access**.
  - **File modified** event subtypes: **File read**, **Hard link created**, **Symbolic link created**.
  - **Registry modified** event subtypes: **Registry key renamed**, **Registry key saved**.
  - New fields for the **Module loaded** and **Connection to remote host** events.
- Expanded functionality for the Endpoint Agent represented by Kaspersky Endpoint Security 12.2 for Linux:
  - Events: **Connection to remote host**, **Port listened**, **Module loaded**, **DNS**, **Process access**.
  - **File modified** event subtype: **File read**.
  - Quarantining an object.
  - Creation of prevention rules.
- Enabling mandatory account password change.
- Scanning of encrypted archives downloaded from an URL in an email message.
- Applying response actions to multiple devices.
- NDR functionality:
  - Viewing network traffic events.
  - Alerts based on the External Analysis technology.
  - Inventory of devices on the local network of the organization.
  - Viewing the following types of device information:
    - User accounts registered in the operating systems of the devices.
    - File execution on devices.
    - Address spaces of devices.
  - Displaying risks associated with devices.
  - Dynamic IP addressing of devices.
  - Monitoring the network activity of devices on the network map.
  - Actively polling devices to enrich information in the list of devices and build the network topology map.
  - Network session analysis.

- Identifying the name of the transport protocol used in the network session.
- Identifying the name of the application layer protocol used in the network session.
- Finding sessions by network packets in the traffic storage, as well as downloading the data of individual network packets and sessions to a file.
- New types of reports.

Kaspersky Anti Targeted Attack Platform 7.1

- Now you can use a Storage Area Network (SAN) system as a drive for storing the data of a Central Node component installed on a server.
- **USB device** event type.
- Selecting the **Last week** period when searching for events in the **Threat Hunting** section.
- Tracking of failed authentication attempts in the web interface or management console of the Central Node or Sandbox components.
- Termination of inactive user sessions in the web interface or management console of the Central Node, Sensor, or Sandbox components after a specified duration.
- When adding an Intrusion Detection rule from Kaspersky to an exclusion, specifying the conditions when you want it to apply. For example, you can apply exclusions only to selected hosts.
- Uploading information about network traffic alerts and events (NDR events) to the GosSOPKA system.
- Limiting the amount of telemetry from the Endpoint Agent component (when integrated with the KEDR functionality).

- The application must be deployed on the Ubuntu Server operating system.
- You can use only KATA and/or KEDR license keys.
- Upgrading the application from version 5.1 to version 7.1 is only possible if the CPU of the Central Node server supports the BMI2, AVX, and AVX2 instruction sets. If these instruction sets are not supported, you can install the application version 7.1.1.

  The upgrade must be performed sequentially from version 5.1: 5.1 → 6.0, 6.0 → 6.0.2, 6.0.2 → 6.1, 6.1 → 7.0.3, 7.0.3 → 7.1.1 or 7.1.2.

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).

When calculating hardware requirements for the server with the Sensor component, please keep in mind that one instance of Kaspersky Endpoint Agent for Linux generates the same load as three instances of Kaspersky Endpoint Agent for Windows.

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 for Windows computers	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

Data type	Disk space (GB)
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.

To avoid possible performance degradation when deploying the application on a virtual platform, we recommend to:

- Set Latency Sensitivity to High.
- Reserve all memory.
- Reserve all CPU.

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 hosts.

  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 host (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 host.

  When calculating the number of hosts with Kaspersky Endpoint Agent, please keep in mind that one instance of Kaspersky Endpoint Agent for Linux generates the same load as three instances of Kaspersky Endpoint Agent for Windows.

  Kaspersky Endpoint Agent for Windows can also be installed on a SCADA server.

If Kaspersky Endpoint Agent for Windows is installed on a SCADA server, the load generated by the program is calculated as follows: one Kaspersky Endpoint Agent for Windows program on a SCADA server generates the same load as 20 Kaspersky Endpoint Agent for Windows programs on a host.

You can use Kaspersky Endpoint Agent for Linux and Kaspersky Endpoint Agent for Windows simultaneously.

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.

Kaspersky Anti Targeted Attack Platform does not support operation with software RAID array.

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 for Windows hosts	Minimum RAM (GB)	Minimum number of logical cores at 3 GHz	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
10,000	160	20	100	1000	1	4	2000	800		10
15,000	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 for Windows hosts	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 (Mbps)	Minimum RAM (GB)	Minimum number of logical cores at 3 GHz	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 s
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	
10,000	2	1000	Not processed	192	40	100	1000	2	4	2000	
5000	5	Not processed	2000	144	20	100	1000	1.9	4	1000	
10,000	20	Not processed	4000	192	36	100	1000	1.9	4	2000	
15,000	20	Not processed	4000	256	48	100	1000	1.9	4	2000	

Example calculations of required server configuration for Kaspersky Anti Targeted Attack Platform components

If you want to:

- process traffic from a network device with a throughput up to 4 Gbps
- process 20 email messages per second
- use 15,000 hosts with Kaspersky Endpoint Agent for Windows **or** 5000 hosts with Kaspersky Endpoint Agent for Linux,

you need two servers with the following hardware:

- Server with the Central Node component: at least 256 GB RAM and at least 48 logical CPU cores
- Server with the Sensor component: at least 32 GB RAM and at least 48 logical CPU cores

The above calculation is also valid for an infrastructure with 5000 hosts with Kaspersky Endpoint Agent for Linux or a combination of components (for example, 9000 hosts with Kaspersky Endpoint Agent for Windows and 2000 hosts with Kaspersky Endpoint Agent for Linux).

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 2,000 GB of free space on the first disk subsystem and at least 2,400 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 Kaspersky Endpoint Agent for Windows hosts>/15,000 * (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

Maximum 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 10 SCN servers under heavy load are listed in the table below.

Hardware requirements for the PCN server

Maximum number of Kaspersky Endpoint Agent for Windows hosts	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 subsyste		
					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 disk arra size (TB
10,000	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
10,000	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 the Endpoint Agent component and the server with the Central Node component are presented in the table below.

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

Maximum number of Kaspersky Endpoint Agent for Windows hosts	Required link bandwidth reserved for Endpoint Agent for Windows components (Mbps)
10	1
50	2
100	3
1000	20
10,000	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 for Windows hosts	Maximum number of email messages per second	Maximum volume of traffic from SPAN ports (Mbps)	Required communication channel bandwidth (Mbps)
5000	5	2000	20
10,000	20	4000	30

Hardware requirements for Central Node cluster servers

A cluster must include at least 4 servers: 2 storage servers and 2 processing servers. To process traffic from 15,000 hosts with Kaspersky Endpoint Agent, you need at least 2 storage servers and 2 processing servers. To process traffic from 30,000 hosts with Kaspersky Endpoint Agent, you need at least 2 storage servers and 3 processing servers.

Each cluster server must have two network adapters to configure cluster and external subnet. The cluster subnet must operate at 10 Gbit/s. The external subnet must operate at 1 Gbit/s.

For a clustered subnet, the following requirements must also be met:

- A cluster subnet must include only the cluster servers and network switches.
- The cluster servers must all be in the same L1 or L2 segment. To do this, you can connect all the servers in the cluster to a single network switch or use software tunneling. For example, L2TPv3 or Overlay Transport Virtualization (OTV).
- The "network latency" value must meet the "single digit latency" requirement, that is, the value must be less than 10 milliseconds.

The hardware requirements for cluster servers when using KEDR functionality are listed in the table below.

Hardware requirements for processing servers when using KEDR functionality

Minimum RAM (GB)	Minimum number of logical cores	RAID disk array type	The number of disks in a RAID disk array	Single HDD volume (GB)
256	48	RAID 1	2	1200

Hardware requirements for storage servers when using KEDR functionality

Minimum RAM (GB)	Minimum number of logical cores	First disk subsystem			Second disk subsystem	
		RAID disk array type	The number of disks in a RAID disk array	Single HDD volume (GB)	Number of disks	Single HDD volume (GB)
128	16	RAID 1	2	1200	6	1200

The performance requirements for disk subsystems are equivalent to those specified in the table *Hardware requirements for a server with the Central Node component when using KEDR functionality* (see above).

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. Run the data recording script by executing the following commands:

   ```
   kata-collect --output-dir path-to-folder
   ```

   ```
   --output-dir <path to directory>
   ```

   When the script finishes running, the *collect.tar.gz* archive will be moved to the specified directory.

3. Forward this archive to Kaspersky Lab staff 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 for Windows computers	Number of physical servers with the Sandbox component	
			When using three images of Windows OS	When using three images of Windows OS and one image of Linux OS
1	200	1000	1	1
2	500	3000	1	1
1	1000	5000	1	1
5	2000	5000	1	1
20	4000	10000	2	3

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) processor at 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 application

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

A number of limitations apply to components. We recommend understanding these before installing the application.

Preparing for installing application 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 purpose of 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 server hosting the Central Node component on the following ports:

      - TCP 22 for connection to the server via SSH.
      - TCP 443 for receiving data from computers with Kaspersky Endpoint Agent.
      - TCP 8443 for viewing scan results in the program web interface.

   b. Allow outbound connections to the following ports for the server hosting the Central Node component:

      - TCP 80, 443 and 1443 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.

   b. Allow outbound connections to the following ports for the server hosting the Sensor component:

      - TCP 80 and 443 for communication with servers of the KSN service and Kaspersky update servers.
      - TCP 995 (or TCP 110 for unprotected connections) for integration with a mail server.

   If you install an additional 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. 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.

6. If you are using the distributed solution and multitenancy mode, prepare the corporate IT infrastructure for installation of the Central Node components as follows:

   a. Allow inbound connection to port 8443 for the server with the PCN role.

   b. 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 sending 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. Run the VMware ESXi hypervisor.

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

Installing and configuring the program involves the following steps:

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

   You can install the Central Node and Sensor components in one of the following configurations:

   - Cluster.
   - Server.

   If there are multiple Central Node components, you can use the program in distributed solution mode.
5. Installing the Sensor component

   If there are multiple Sensor components, you can install and configure the Sensor component on the necessary number of servers.
6. Configuring the Central Node and Sensor components
7. **Installing Kaspersky Endpoint Agent for Windows or Kaspersky Endpoint Agent for Linux on computers in the corporate IT infrastructure**

   You can use Kaspersky Endpoint Agent in the following configurations:

   - Without integration with the EPP program.

     In this case, you only need to install Kaspersky Endpoint Agent for Windows or Kaspersky Endpoint Agent for Linux.
   - With integration with the EPP program.

     In this case, Kaspersky Endpoint Agent also sends information about threats detected by the EPP program and results of threat processing by this program to the Central Node server.

   Kaspersky Endpoint Agent for Windows can integrate with the following EPP programs:

   - Kaspersky Endpoint Security for Windows.

     Integration of Kaspersky Endpoint Agent for Windows with Kaspersky Endpoint Security for Windows

To integrate these programs, you must install Kaspersky Endpoint Agent as part of Kaspersky Endpoint Security. Integrating separately installed programs is not supported.

To install Kaspersky Endpoint Agent as part of Kaspersky Endpoint Security:

1. Start the installation of the Kaspersky Endpoint Security program, which includes Kaspersky Endpoint Agent in its distribution kit.

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

2. During installation, select the Endpoint Agent component.

   After the program with the Endpoint Agent component is installed, the list of installed programs includes Kaspersky Endpoint Security and Kaspersky Endpoint Agent.

If necessary, you can upgrade the Kaspersky Endpoint Agent that is already installed as part of Kaspersky Endpoint Security. Integration between compatible versions of the programs is maintained both when Kaspersky Endpoint Agent is upgraded and when Kaspersky Endpoint Security is upgraded. You can upgrade a previous version of Kaspersky Endpoint Agent to version 3.12 only for Kaspersky Endpoint Agent version 3.7 or later.

- Kaspersky Security for Windows Server.

  Integration of Kaspersky Endpoint Agent for Windows with Kaspersky Security for Windows Server

  To integrate these programs, you must install Kaspersky Endpoint Agent as part of Kaspersky Security for Windows Server. Integrating separately installed programs is not supported.

  To install Kaspersky Endpoint Agent as part of Kaspersky Security for Windows Server:

  1. Start the installation of the Kaspersky Security for Windows Server program, which includes Kaspersky Endpoint Agent in its distribution kit.

     For more details about installing Kaspersky Security for Windows Server, see *Kaspersky Security for Windows Server Help*.

  2. During installation, select the Kaspersky Endpoint Agent component.

     After the program with the Kaspersky Endpoint Agent component is installed, the list of installed programs includes Kaspersky Security for Windows and Kaspersky Endpoint Agent.

  If necessary, you can upgrade the Kaspersky Endpoint Agent that is already installed as part of Kaspersky Security for Windows Server. Integration between compatible versions of the programs is maintained both when Kaspersky Endpoint Agent is upgraded and when Kaspersky Security for Windows Server is upgraded.

- Kaspersky Security for Virtualization Light Agent.

  Integration of Kaspersky Endpoint Agent for Windows with Kaspersky Security for Virtualization Light Agent

  Kaspersky Endpoint Agent and Kaspersky Security for Virtualization Light Agent are installed separately. Kaspersky Endpoint Agent cannot be installed as part of Kaspersky Security for Virtualization Light Agent.

To enable the integration of Kaspersky Endpoint Agent with Kaspersky Security for Virtualization Light Agent:

1. Install Kaspersky Security for Virtualization Light Agent if it has not been installed yet.
2. Enable the integration of Light Agent with Kaspersky Endpoint Agent.

   You can enable the integration with Kaspersky Endpoint Agent during installation or upgrade of Light Agent. You can also enable the integration with Kaspersky Endpoint Agent using the procedure for modifying the set of installed components of Light Agent.

   For more details about installing, enabling integration, and updating the program, as well as about the procedure for modifying the set of installed components, see *Kaspersky Security for Virtualization Light Agent Help*.
3. Install Kaspersky Endpoint Agent on the virtual machine with Light Agent, if it has not been installed yet.

> For integration with Kaspersky Security for Virtualization Light Agent 5.2, we recommend using Kaspersky Endpoint Agent 3.12. If necessary, you can upgrade the Kaspersky Endpoint Agent program and Kaspersky Security for Virtualization Light Agent. When you upgrade the programs, integration between compatible versions is maintained.

- Kaspersky Industrial CyberSecurity for Nodes.

  Integration of Kaspersky Endpoint Agent for Windows with Kaspersky Industrial CyberSecurity for Nodes

  To enable integration of Kaspersky Endpoint Agent with Kaspersky Industrial CyberSecurity for Nodes:

  1. Install Kaspersky Industrial CyberSecurity for Nodes if the program has not been installed yet.

     For more details on installation, see *Kaspersky Industrial CyberSecurity for Nodes Help*.
  2. Install Kaspersky Endpoint Agent on the same device if it has not been installed yet.

  The applications are integrated automatically.

> To integrate with Kaspersky Industrial CyberSecurity for Nodes, the corresponding license key must be installed in the Kaspersky Endpoint Agent.

For detailed information, you can contact your account manager.

Kaspersky Endpoint Agent for Linux can integrate with the Kaspersky Endpoint Security for Linux EPP system.

Integration of Kaspersky Endpoint Agent for Linux with Kaspersky Endpoint Security for Linux

To integrate Kaspersky Endpoint Agent for Linux with Kaspersky Endpoint Security for Linux, you can use separately installed programs.

To enable the integration of Kaspersky Endpoint Agent with Kaspersky Endpoint Security:

1. Install Kaspersky Endpoint Security.

   For more details about installing the program, see *Kaspersky Endpoint Security for Linux Help*.

2. Do the following:

   a. If Kaspersky Endpoint Agent has not been installed yet, install Kaspersky Endpoint Agent.

      The integration between programs is enabled automatically.

   b. If Kaspersky Endpoint Agent has already been installed, enable the integration between programs.

      To do so, you must enable the recording of event information in syslog for Kaspersky Endpoint Security for Linux.

      For more details about configuring the program, see *Kaspersky Endpoint Security for Linux Help*.

If necessary, you can upgrade Kaspersky Endpoint Agent and Kaspersky Endpoint Security for Linux. When you upgrade the programs, integration between compatible versions is maintained.

Installing the Sandbox component

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

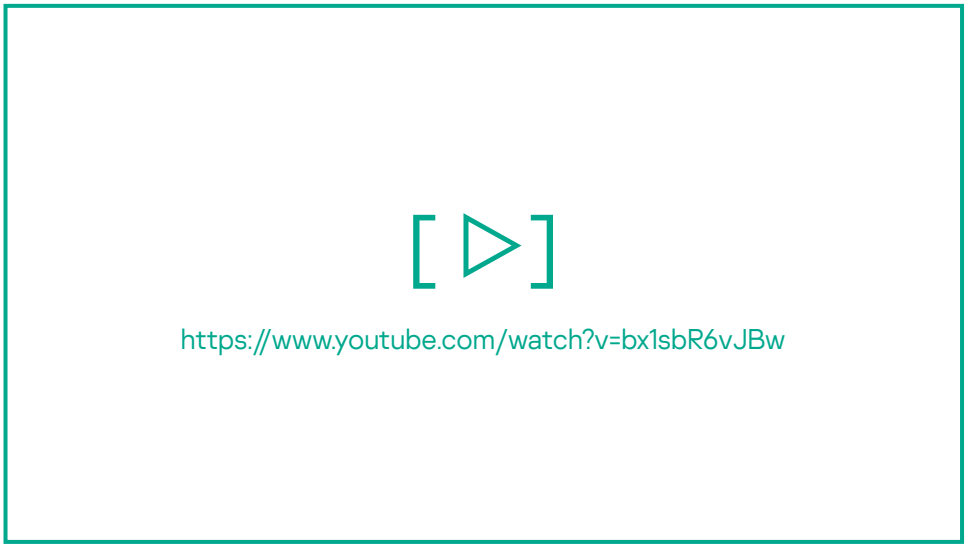
To begin the installation of the Sandbox component:

1. Run the disk image containing the Sandbox component.

   The Setup Wizard starts.

2. Select **Continue** and press **ENTER**.

Watch a video tutorial on deploying the Sandbox component. You can play the video on the Help page (see below) or follow the link https://youtu.be/bx1sbR6vJBw?si=D1PrZ5o4vwlxaNoP.



Deploying the Sandbox component

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

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

Assign a server host name to be used by DNS servers.

To assign the host name for a server:

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 controlling network interface in the list

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

- 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.

Select the network interface that you want to use as the controlling interface.

To select the management 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 management 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

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 a Sandbox administrator account:

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 account.

   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.

Deploying the Central Node component with Embedded Sensor as a cluster

A cluster must include at least 4 servers: 2 storage servers and 2 processing servers. You can use the Sizing Guide determine the right number of servers for your organization.

Deployment of the Central Node component with Embedded Sensor in the form of a cluster includes the following steps:

1. **Deploying the first storage server**

   The first step is to deploy the storage server. After the storage server is deployed, you can add additional storage and processing servers to the cluster.

2. **Deploying processing servers and additional storage servers**

   You can deploy the servers in any order.

3. **Configuring the sizing settings of the application**

   At the final stage of cluster deployment, you need to configure the scaling settings of the application: specify the planned volume of SPAN traffic, email traffic, the number of hosts with the Endpoint Agent component, as well as the size of the Storage and event database.

   Immediately after installing the application, we recommend configuring (enabling or leaving disabled) the mandatory password change after the first successful authentication.

If you have a cluster deployed on physical servers and want to add more hard drives to these servers or replace some of the existing drives and then reinstall the cluster, you must purge the drives previously allocated for the OSD (Object Storage Daemon) on the storage servers before installing components. Otherwise, the application is not guaranteed to work correctly. If you want to completely disconnect the drives and no longer plan to reconnect them to the server, purging the drives is not necessary.

Deploying a storage server

To deploy a data storage server, you need to run a disk image with the Central Node and Sensor components.

If an error occurred while performing the steps of the Setup Wizard, contact Technical Support.

Step 2. Selecting a server role

To select a server role:

1. Select one of the following options:

   - **storage**.

     This role is for installing a storage server for deploying the Central Node component as a cluster.

- **processing**.

  This role is for installing a processing server for deploying the Central Node component as a cluster.

  > The role also includes the installation and configuration of the Sensor component.

- **single**.

  This role is for installing the Central Node and Sensor components on the same server.

- **sensor**.

  This role is for installing the Sensor component on a standalone server.

2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 3. Selecting the deployment mode

To select a deployment mode:

1. Select one of the following options:

   - **First node installation**.

     Select this value when deploying the first server in the cluster.

   - **Add extra node to the cluster**.

     Select this value when deploying a server that will be added to an existing cluster.

2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 4. Selecting a disk for installing the component

You need at least 150 GB of disk space. If less than 150 GB of disk space is available, installation finishes with an error.

To select a disk for installing the component:

1. Select one of the suggested drives for installing the component and press **Enter**.

   The confirmation window is displayed.

2. Select **Yes** and press **Enter**.

The Setup Wizard proceeds to the next step.

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

To proceed with the installation, you must read and accept the terms and conditions of the End User License Agreement and the Privacy Policy of AO Kaspersky Lab (hereinafter also referred to as the "End User License Agreement" and the "Privacy Policy" respectively). Installation will not continue until you accept the terms of the End User License Agreement and Privacy Policy.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Ubuntu operating system:

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

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

2. Please read the End User License Agreement.

   To move up and down, you can use the keys: **↑, ↓, PageUp**, and **PageDown**.

3. If you accept the End User License Agreement, select **I accept** and press **Enter**.

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

4. Please carefully read the Privacy Policy.

5. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Astra Linux operating system:

1. Select the language for viewing the End User License Agreement for Astra Linux operating systems, the End User License Agreement, and the Privacy Policy in the list and press the **Enter** key.

   To move up and down, you can use the keys: ↑, ↓, **PageUp**, and **PageDown**.

   This opens a window with the text of the Astra Linux End User License Agreement.

2. Read the End User License Agreement of the Astra Linux operating systems.

3. If you accept the terms and conditions of the End User License Agreement of Astra Linux operating systems, select **I accept** and press **Enter**.

   This opens a window with the text of the AO Kaspersky Lab End User License Agreement.

4. Please read the End User License Agreement.

5. If you accept the terms and conditions of the End User License Agreement, select **I accept** and press **Enter**.

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

6. Please carefully read the Privacy Policy.

7. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 5. Selecting a network mask for server addressing

We recommend using the default value.

The netmask may not match netmasks used in the organization's infrastructure.

To specify the network mask for server addressing:

- If you want to use the predefined value for the network mask, select the **Ok** button and press **Enter**.

  Default value: 198.18.0.0/16.

- If you want to specify a different network mask, in the **Subnet** field, enter your value, select the **Ok** button, and press **Enter**.

  The mask must match the template: x.x.0.0/16.

The Setup Wizard proceeds to the next step.

Step 6. Selecting a network mask for addressing of application components

We recommend using the default value.

The network for application component addressing must not overlap with the network for cluster server addressing.

To specify the network mask for addressing the main components of the application:

- If you want to use the predefined value for the network mask, select the **Ok** button and press **Enter**.

  Default value: 198.19.0.0/16.

- If you want to specify a different network mask, in the **Bridge/overlay subnets** field, enter your value, select the **Ok** button, and press **Enter**.

  The mask must match the template: x.x.0.0/16.

The Setup Wizard proceeds to the next step.

Step 7. Selecting the cluster network interface

The cluster network interface is used for communication between cluster servers.

To select the cluster network interface:

1. Select the row containing the network interface that is used for the internal network.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.
2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 8. Selecting the external network interface

The external network interface is used for SSH access to the server, managing the web interface of Kaspersky Anti Targeted Attack Platform, and other external connections.

To select the external network interface:

1. Select the row containing the network interface that is used for the external network.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.
2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 9. Selecting the method of obtaining IP addresses for network interfaces

To select a method for obtaining an IP address for network interfaces:

1. Select the row containing the **Configuration type:** and press **Enter**.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.
2. In the opened window, select one of the following options:
   - **dhcp**.
   - **static**.
3. If you selected **static**:
   a. Select the row containing the parameter and press the **Enter** key.
   b. This opens a window; in that window, enter the required information.

   > You need to specify a value for each parameter.

4. Select **OK**.

5. Press **Enter**.

   The Setup Wizard proceeds to the next step.

Step 10. Creating an administrator account and authenticating the server in the cluster

During this step, you need to do one of the following:

- Create an administrator account if you are deploying the first server in the cluster.
- Authenticate a server in the cluster if you are deploying additional storage servers.

Creating the administrator account

> An administrator account is only required when deploying the first server in the cluster. If you are deploying an additional storage server, instead of opening a window that prompts you to create an administrator account, the application prompts you to authenticate the server in the cluster.

When deploying the first server in the cluster, you need to create an administrator account. This user account is used for managing the web interface of the application, the administrator menu of the application, and for managing the application in Technical Support Mode.

By default, the user name of the administrator account is *admin*. You must enter a password for that user account.

To enter a password for the administrator user account:

1. This opens a window; in that window, in the **min length** field, enter the minimum password length. You must enter a value of 8 or greater.

2. Select **Ok** and press **Enter**.

   This opens the password creation window.

3. This opens a window; in that window, in the **password** field, enter the password for the administrator account.

   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.

4. In the **confirm** field, enter the password again.

5. Select **Ok** and press **Enter**.

   The Setup Wizard proceeds to the next step.

Authenticating the server in the cluster

Authenticating a server in the cluster is only required when deploying additional storage servers. If you are deploying the first server in the cluster, the application prompts you to create an administrator account instead of authenticating the server.

To authenticate a server in the cluster, you need to enter the admin account password that was set when the first server in the cluster was deployed.

To authenticate a server in the cluster:

1. In the **password** field, enter the password for the administrator account.
2. Select **Ok** and press **Enter**.

   To select a button, you can use the ↑, ↓, PageUp, and PageDown keys.

The server in the cluster will be authenticated. The Setup Wizard proceeds to the next step.

Step 11. Adding DNS server addresses

This step is available if you are deploying the first server in the cluster.

Configure the DNS settings for the operation of servers with application components.

To add DNS server addresses:

1. Select the **Add** field and press **Enter**.
2. Enter the IP address of the DNS server in the IPv4 format.
3. Select **OK** and press **Enter**.
4. If you want to add the IP address of an additional DNS server, repeat steps 1 through 3 of these instructions.
5. Having added all DNS servers, select **Continue** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 13. Selecting disks for the Ceph storage

Select the disks for the Ceph storage. The number of disks is determined in accordance with the sizing guide.

To select disks for the Ceph storage:

1. Select the row containing the required drive.

   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.

2. Press **Enter**.

3. Repeat steps 1 to 2 to select more drives if you want to select multiple drives.

4. Select the **Apply and finish** field and press **Enter**.

   The confirmation window is displayed.

5. Select **Yes** and press **Enter**.

The configuration may take some time. Then the installation is complete. You can proceed to configure the servers of the cluster.

Deploying the processing server

To deploy a processing server, you need to run a disk image with the Central Node and Sensor components.

If an error occurred while performing the steps of the Setup Wizard, contact Technical Support.

Step 2. Selecting a server role

To select a server role:

1. Select one of the following options:

   - **storage**.

     This role is for installing a storage server for deploying the Central Node component as a cluster.

   - **processing**.

     This role is for installing a processing server for deploying the Central Node component as a cluster.

     The role also includes the installation and configuration of the Sensor component.

   - **single**.

     This role is for installing the Central Node and Sensor components on the same server.

   - **sensor**.

     This role is for installing the Sensor component on a standalone server.

2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 2. Selecting the deployment mode

To select a deployment mode:

1. Enter one of the following numbers:

   - **1**.

     Select this value when deploying the first server in the cluster.

   - **2**.

     Select this value when deploying a server that will be added to an existing cluster.

2. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 3. Selecting a disk for installing the component

To select a disk for installing the component:

1. Enter the number of the relevant disk.
2. Press **ENTER**.
3. Do the following:

   - Enter **y** if you want to confirm the drive selection.
   - Enter **n** if you want to select a different drive.

4. If you selected **n**, repeat steps 1-2 of these instructions.

The Setup Wizard proceeds to the next step.

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

To proceed with the installation, you must read and accept the terms and conditions of the End User License Agreement and the Privacy Policy of AO Kaspersky Lab (hereinafter also referred to as the "End User License Agreement" and the "Privacy Policy" respectively). Installation will not continue until you accept the terms of the End User License Agreement and Privacy Policy.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Ubuntu operating system:

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

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

2. Please read the End User License Agreement.

   To move up and down, you can use the keys: ↑, ↓, **PageUp**, and **PageDown**.

3. If you accept the End User License Agreement, select **I accept** and press **Enter**.

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

4. Please carefully read the Privacy Policy.

5. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Astra Linux operating system:

1. Select the language for viewing the End User License Agreement for Astra Linux operating systems, the End User License Agreement, and the Privacy Policy in the list and press the **Enter** key.

   To move up and down, you can use the keys: ↑, ↓, **PageUp**, and **PageDown**.

   This opens a window with the text of the Astra Linux End User License Agreement.

2. Read the End User License Agreement of the Astra Linux operating systems.

3. If you accept the terms and conditions of the End User License Agreement of Astra Linux operating systems, select **I accept** and press **Enter**.

   This opens a window with the text of the AO Kaspersky Lab End User License Agreement.

4. Please read the End User License Agreement.

5. If you accept the terms and conditions of the End User License Agreement, select **I accept** and press **Enter**.

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

6. Please carefully read the Privacy Policy.

7. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 5. Selecting a network mask for server addressing

We recommend using the default value.

The netmask may not match netmasks used in the organization's infrastructure.

To specify the network mask for server addressing:

- If you want to use the predefined value for the network mask, select the **Ok** button and press **Enter**.

  Default value: 198.18.0.0/16.

- If you want to specify a different network mask, in the **Subnet** field, enter your value, select the **Ok** button, and press **Enter**.

  The mask must match the template: x.x.0.0/16.

The Setup Wizard proceeds to the next step.

Step 6. Selecting a network mask for directing program components

During this step, you need to specify the network mask for directing the main program components (services) that will operate on servers with the Central Node component.

> The network for directing application components must not overlap with the network for directing the cluster servers.

To specify the network mask for directing the main components of the program:

- If you want to use the predefined value for the network mask, press **Enter**.

  Default value: 198.19.0.0/16.

- If you want to specify a different network mask, enter the value and press **Enter**.

  The mask must match the template: x.x.0.0/16.

The Setup Wizard proceeds to the next step.

Step 7. Selecting the cluster network interface

The cluster network interface is used for communication between cluster servers.

To select the cluster network interface:

1. Select the row containing the network interface that is used for the internal network.

   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys. The selected row is highlighted in red.

2. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 8. Selecting the external network interface

The external network interface is used for SSH access to the server, managing the web interface of Kaspersky Anti Targeted Attack Platform, and other external connections.

To select the external network interface:

1. Select the row containing the network interface that is used for the external network.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys. The selected row is highlighted in red.
2. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 9. Selecting the method of obtaining IP addresses for network interfaces

To select a method for obtaining an IP address for network interfaces:

1. Select the row containing the **Configuration type:** and press **Enter**.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys. The selected row is highlighted in red.
2. In the opened window, select one of the following options:
   - **dhcp**.
   - **static**.
3. If you selected **static**:
   a. Select the row containing the parameter and press the **Enter** key.
   b. In the opened window, enter the required data and press **Enter** twice.

   > You need to specify a value for each parameter.
4. Select the row containing **Save**.
5. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 9. Authenticating the server in the cluster

To authenticate a server in the cluster, you need to enter the admin account password that was set when the first server in the cluster was deployed.

To authenticate a server in the cluster:

1. In the **password** field, enter the password for the administrator account.
2. Select **Ok** and press **Enter**.

   To select a button, you can use the ↑, ↓, PageUp, and PageDown keys.

The server in the cluster will be authenticated. The Setup Wizard proceeds to the next step.

Configuring receipt of mirrored traffic from SPAN ports

For the application to work correctly, receipt of mirrored traffic from SPAN ports must be enabled on one of the processing servers in the cluster. If you do not actually need to process mirrored traffic from SPAN ports, specify 0 for SPAN traffic when configuring sizing.

Mirror traffic processing must be enabled on only one processing server in the cluster.

To turn on the receipt of mirrored traffic from SPAN ports:

In the window that is displayed, select **Yes** and press **Enter**.

The configuration may take some time. Then the installation is complete. For the application to work correctly, you must configure the server.

To turn off the receipt of mirrored traffic from SPAN ports:

In the opened window, select **No** and press **Enter**.

The configuration may take some time. Then the installation is complete. For the application to work correctly, you must configure the server.

Step 12. Adding DNS server addresses

Configure the DNS settings for the operation of servers with program components.

To add DNS server addresses:

1. Enter the IP address of the primary DNS server in IPv4 format.

   You must enter at least one DNS server address.

2. If you want to add the IP address of an additional DNS server, press **Enter** and enter the address of the server.
3. Having added all DNS servers, press **Enter** twice.

Installation is complete. You can proceed to the configuration of cluster servers in the web interface for sizing management.

Installing the Central Node component with Embedded Sensor on a server

Installing the Central Node component with Embedded Sensor on the server involves the following steps:

1. **Installing the Central Node component with Embedded Sensor**

   To install the component on the physical server, you need to boot from a disk image with the Central Node and Sensor components.

   To install the component on a virtual server, you need to connect the disk image with the Central Node and Sensor components to the selected virtual machine and run it. The installation starts immediately after the virtual machine is turned on. You can manage the installation process using the console of the virtual machine.

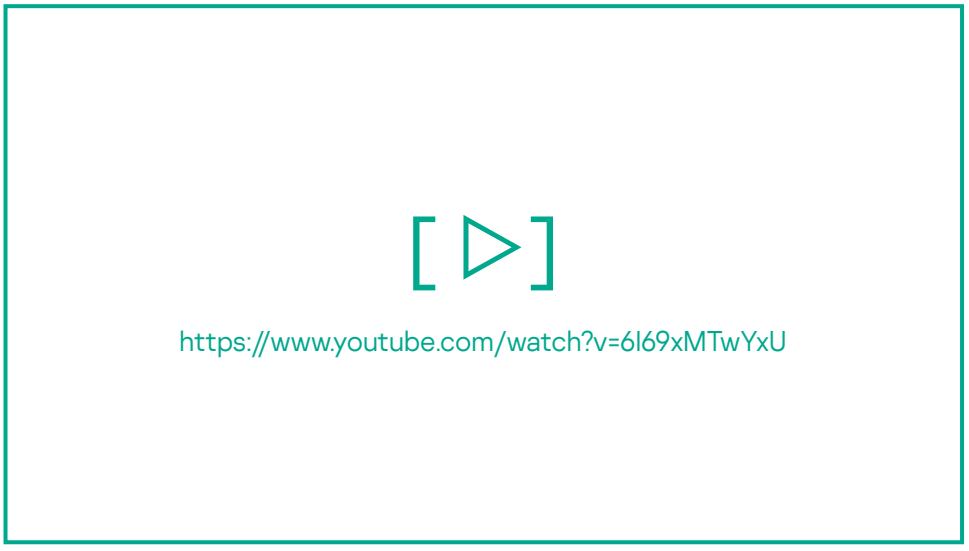
2. **Configuring the sizing settings of the application**

   At the final stage of cluster deployment, you need to configure the scaling settings of the application: specify the planned volume of SPAN traffic, email traffic, the number of hosts with the Endpoint Agent component, as well as the size of the Storage and event database.

   Immediately after installing the application, we recommend configuring (enabling or leaving disabled) the mandatory password change after the first successful authentication.

If an error occurred while performing the steps of the Setup Wizard, contact Technical Support.

Watch a video tutorial on deploying the Central Node component. You can play the video on the Help page (see below) or follow the link https://youtu.be/6l69xMTwYxU?si=lQU1mWrchjvZmuQW.



Deploying the Central Node component

Step 2. Selecting a server role

To select a server role:

1. Select one of the following options:

   - **storage**.

     This role is for installing a storage server for deploying the Central Node component as a cluster.

   - **processing**.

     This role is for installing a processing server for deploying the Central Node component as a cluster.

     > The role also includes the installation and configuration of the Sensor component.

   - **single**.

     This role is for installing the Central Node and Sensor components on the same server.

   - **sensor**.

     This role is for installing the Sensor component on a standalone server.

2. Press **Enter**.

The Setup Wizard proceeds to the next step.

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

To proceed with the installation, you must read and accept the terms and conditions of the End User License Agreement and the Privacy Policy of AO Kaspersky Lab (hereinafter also referred to as the "End User License Agreement" and the "Privacy Policy" respectively). Installation will not continue until you accept the terms of the End User License Agreement and Privacy Policy.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Ubuntu operating system:

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

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

2. Please read the End User License Agreement.

   To move up and down, you can use the keys: **↑**, **↓**, **PageUp**, and **PageDown**.

3. If you accept the End User License Agreement, select **I accept** and press **Enter**.

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

4. Please carefully read the Privacy Policy.
5. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Astra Linux operating system:

1. Select the language for viewing the End User License Agreement for Astra Linux operating systems, the End User License Agreement, and the Privacy Policy in the list and press the **Enter** key.

   To move up and down, you can use the keys: ↑, ↓, **PageUp**, and **PageDown**.

   This opens a window with the text of the Astra Linux End User License Agreement.
2. Read the End User License Agreement of the Astra Linux operating systems.
3. If you accept the terms and conditions of the End User License Agreement of Astra Linux operating systems, select **I accept** and press **Enter**.

   This opens a window with the text of the AO Kaspersky Lab End User License Agreement.
4. Please read the End User License Agreement.
5. If you accept the terms and conditions of the End User License Agreement, select **I accept** and press **Enter**.

   This opens a window displaying the text of the Privacy Policy.
6. Please carefully read the Privacy Policy.
7. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 3. Selecting a disk for installing the component

You need at least 150 GB of disk space. If less than 150 GB of disk space is available, installation finishes with an error.

A SAN storage system cannot be used as a component installation drive.

To select a disk for installing the component:

1. Select one of the suggested drives for installing the component and press **Enter**.

   The confirmation window is displayed.
2. Select **Yes** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 4. 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 allocate the disk for the Targeted Attack Analyzer component's database:

1. Select one of the suggested drives for the Targeted Attack Analyzer component database.

   If you do not need the database of the Targeted Attack Analyzer component, select **Do not allocate a separate disk for TAA** line.

2. In the confirmation window, select **Yes** and press **Enter**.

   The Setup Wizard proceeds to the next step.

If you want to use a SAN data storage system, do one of the following:

- If the SAN is connected to a physical or virtual server, at this step of the installation process, select the SAN, which appears as a local disk, as the storage disk.

  Instructions for connecting a SAN are provided by its vendor.

- If a network interface is used for access to the SAN:

  1. At this step of the installation process, select **Do not allocate a separate disk for TAA.**
  2. Contact Technical Support for instructions on changing the mount point of the second disk subsystem.
  3. Complete the remaining steps of the Central Node with Embedded Sensor installation wizard on the server.
  4. In Technical Support Mode, change the mount point in accordance with the instructions you received.

Step 5. Selecting a network mask for cluster server addressing

To specify the network mask for cluster server addressing:

- If you want to use the predefined value for the network mask, press **Enter**.

  Default value: 198.18.0.0/16.

- If you want to specify a different network mask, enter the value and press **Enter**.

  The mask must match the template: x.x.0.0/16.

The Setup Wizard proceeds to the next step.

Step 7. Selecting the external network interface

The external network interface is used for SSH access to the server, managing the web interface of Kaspersky Anti Targeted Attack Platform, and other external connections.

To select the external network interface:

1. Select the row containing the network interface that is used for the external network.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.
2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 8. Selecting the method of obtaining IP addresses for network interfaces

To select a method for obtaining an IP address for network interfaces:

1. Select the row containing the **Configuration type:** and press **Enter**.
   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.
2. In the opened window, select one of the following options:
   - **dhcp**.
   - **static**.
3. If you selected **static**:
   a. Select the row containing the parameter and press the **Enter** key.
   b. This opens a window; in that window, enter the required information.

   > You need to specify a value for each parameter.

4. Select **OK**.
5. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 9. Creating the administrator account

The administrator account is used for managing the web interface of the application, the administrator menu of the application, and for managing the application in Technical Support Mode.

By default, the user name of the administrator account is *admin*. You must enter a password for that user account.

To enter a password for the administrator user account:

1. This opens a window; in that window, in the **min length** field, enter the minimum password length. You must enter a value of 8 or greater.
2. Select **Ok** and press **Enter**.

   This opens the password creation window.
3. This opens a window; in that window, in the **password** field, enter the password for the administrator account.

   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.
4. In the **confirm** field, enter the password again.
5. Select **Ok** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 11. Adding DNS server addresses

Configure the DNS settings for the operation of servers with application components.

To add DNS server addresses:

1. Select the **Add** field and press **Enter**.
2. Enter the IP address of the DNS server in the IPv4 format.
3. Select **OK** and press **Enter**.
4. If you want to add the IP address of an additional DNS server, repeat steps 1 through 3 of these instructions.
5. Having added all DNS servers, select **Continue** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 10. Configuring receipt of mirrored traffic from SPAN ports

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

To turn on receipt of mirrored traffic from SPAN ports:

1. Enter **y**.
2. Press **ENTER**.

   The Setup Wizard proceeds to the next step.

To turn off receipt of mirrored traffic from SPAN ports:

1. Enter **n**.
2. Press **ENTER**.

   The Setup Wizard proceeds to the next step.

Step 12. Configuring time synchronization with an NTP server

Configure synchronization of the server time with the NTP server.

1. Select the **Add** field and press **Enter**.
2. Enter the IP address or name of the NTP server.
3. Select **OK** and press **Enter**.
4. If you want to add the IP address or name of an additional NTP server, repeat steps 1 through 3 of these instructions.
5. Having added all NTP servers, select **Continue** and press **Enter**.

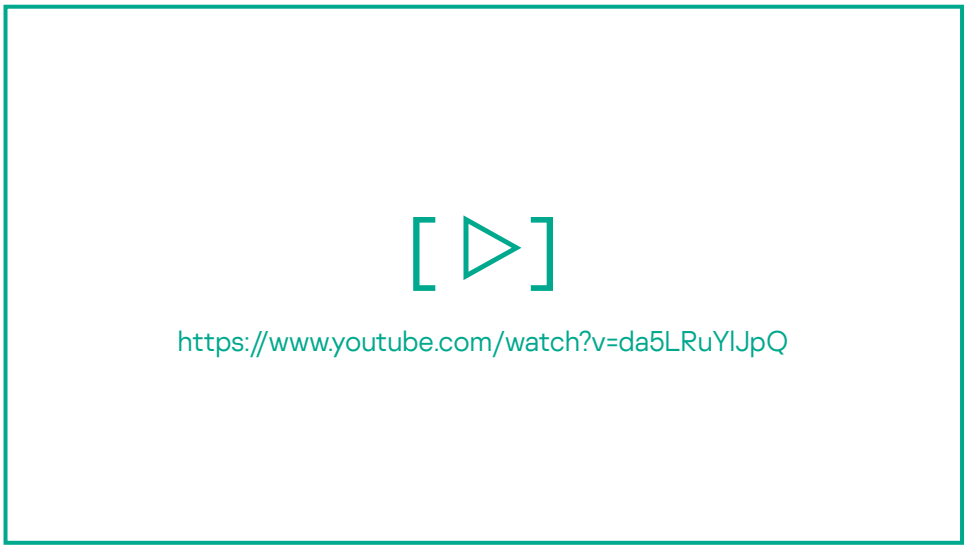
   Installation is complete. For the application to work correctly, you must configure the server.

Installing the Sensor component on a standalone server

To install the Sensor component on a physical server, you need to run a disk image with the Central Node and Sensor components.

To install the Sensor component on a virtual server, you need to connect the disk image with the Central Node and Sensor components to the selected virtual machine and run it. The installation starts immediately after the virtual machine is turned on. You can manage the installation process using the console of the virtual machine.

Watch a video tutorial on deploying the Sensor component. You can play the video on the Help page (see below) or follow the link https://youtu.be/da5LRuYlJpQ?si=JRSPsNRPlK-Jqcfc.



Deploying the Sensor component

Step 2. Selecting a server role

To select a server role:

1. Select one of the following options:

   - **storage**.

     This role is for installing a storage server for deploying the Central Node component as a cluster.

   - **processing**.

     This role is for installing a processing server for deploying the Central Node component as a cluster.

     > The role also includes the installation and configuration of the Sensor component.

   - **single**.

     This role is for installing the Central Node and Sensor components on the same server.

   - **sensor**.

     This role is for installing the Sensor component on a standalone server.

2. Press **Enter**.

The Setup Wizard proceeds to the next step.

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

To proceed with the installation, you must read and accept the terms and conditions of the End User License Agreement and the Privacy Policy of AO Kaspersky Lab (hereinafter also referred to as the "End User License Agreement" and the "Privacy Policy" respectively). Installation will not continue until you accept the terms of the End User License Agreement and Privacy Policy.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Ubuntu operating system:

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

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

2. Please read the End User License Agreement.

   To move up and down, you can use the keys: **↑, ↓, PageUp**, and **PageDown**.

3. If you accept the End User License Agreement, select **I accept** and press **Enter**.

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

4. Please carefully read the Privacy Policy.

5. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

To accept the terms and conditions of the End User License Agreement and the Privacy Policy when installing the components based on the Astra Linux operating system:

1. Select the language for viewing the End User License Agreement for Astra Linux operating systems, the End User License Agreement, and the Privacy Policy in the list and press the **Enter** key.

   To move up and down, you can use the keys: ↑, ↓, **PageUp**, and **PageDown**.

   This opens a window with the text of the Astra Linux End User License Agreement.

2. Read the End User License Agreement of the Astra Linux operating systems.

3. If you accept the terms and conditions of the End User License Agreement of Astra Linux operating systems, select **I accept** and press **Enter**.

   This opens a window with the text of the AO Kaspersky Lab End User License Agreement.

4. Please read the End User License Agreement.

5. If you accept the terms and conditions of the End User License Agreement, select **I accept** and press **Enter**.

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

6. Please carefully read the Privacy Policy.

7. If you accept the terms and conditions of the Privacy Policy, select **I accept** and press **Enter**.

The Setup Wizard proceeds to the next step.

Step 3. Selecting a disk for installing the component

To select a disk for installing the component:

1. Enter the number of the relevant disk.

2. Press **ENTER**.

3. Do the following:

   - Enter **y** if you want to confirm the drive selection.

   - Enter **n** if you want to select a different drive.

4. If you selected **n**, repeat steps 1-2 of these instructions.

The Setup Wizard proceeds to the next step.

Step 6. Selecting the external network interface

The external network interface is used for SSH access to the server, managing the web interface of Kaspersky Anti Targeted Attack Platform, and other external connections.

To select the external network interface:

1. Select the row containing the network interface that is used for the external network.

   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys.

2. Press **Enter**.

The Setup Wizard proceeds to the next step.

Step 5. 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.

   If the Central Node component is deployed as a cluster, you can enter the IP address of any server in the cluster.

2. Press **ENTER**.

The Setup Wizard proceeds to the next step.

Step 6. Creating the administrator account

The administrator account is used to work with the Sensor component in the program administrator menu and in Technical Support Mode.

By default, the user name of the administrator account is *admin*. You must enter a password for that user account.

To enter a password for the administrator user account:

1. In the **password** field, enter the password for the administrator account.

   To select a row, you can use the ↑, ↓, PageUp, and PageDown keys. The selected row is highlighted in red.

2. In the **confirm** field, enter the password again.

3. Select **Ok** and press **Enter**.

The installation will be complete.

Configuring the sizing settings of the program

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 change the operational load on the Central Node component. For example, you can connect additional hosts with Kaspersky Endpoint Agent or servers with the Sensor component to the Central Node component. To do this, you need to specify the planned volume of SPAN traffic, mail traffic, the number of hosts with Kaspersky Endpoint Agent, as well as the size of the Storage and event database. Kaspersky Anti Targeted Attack Platform will determine the optimal configuration of the Central Node servers taking into account the specified settings.

If the Central Node component is deployed as a cluster, the program determines the optimal configuration of all servers in the cluster.

To configure the Central Node servers:

1. Log in to the web interface for sizing management.
2. Go to the **Server configuration** section.
3. In the **Number of Endpoint Agents** field, specify the number of hosts with Kaspersky Endpoint Agent installed that you plan on using.

   If you are not using a KEDR license key, specify 0.
4. In the **Mail traffic, messages per second** field, specify the planned number of emails per second.

   If you are not using a KATA license key, specify 0.
5. In the **SPAN traffic, Mbps** field, specify the planned amount of traffic from SPAN ports on servers with the Sensor component.

   If you are not using a KATA license key, specify 0.
6. In the **Available disk space** section, specify the size of the event database and Storage in one of the following ways:

   - Move the slider separating the **Events database** and **Storage** to the left or right.
   - Specify the values in the **Events database, GB** and **Storage, GB** fields.

   If you are using the non fault-tolerant version of the program, it is recommended to use the default value for the event database field.

   If the Central Node component is deployed as a high availability cluster, use the Sizing Guide to calculate the size of the events database.

Please note that if the disk space allocated to the events database is full, the Central Node component will not receive data from the Endpoint Agent component. If you run out of disk space, make sure you have sized the events database correctly. Kaspersky Anti Targeted Attack Platform does not check the entered values for correctness.

Disk space is automatically reserved for the alert database when the Central Node component is installed.

7. If necessary, you can leave free space on disk by moving the last slider on the right.

8. Click **Configure**.

Kaspersky Anti Targeted Attack Platform will determine the optimal server configuration in accordance with the specified settings and configure the cluster servers. If the configuration is completed successfully, the web interface login window will appear.

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 of the server:

1. In the window of the program web interface, select the **Settings** section, **Certificates** subsection.
2. In the **Server certificate** section, click **Download**.

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 the connection of Central Node, PCN, and SCN to Sandbox.
- Reconfigure traffic forwarding from Endpoint Agent to Sensor and trusted connection with Endpoint Agent.
- Upload a new certificate to Active Directory (if you are using 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 a Central Node server:

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the window of the program web interface, select the **Settings** section, **Certificates** subsection.
3. In the **Server certificate** section, click **Generate**.

   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 application does not support other formats of certificates.

  If you have prepared a certificate in a different format, you must convert it to the 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 the connection of Central Node, PCN, and SCN to Sandbox.
- Reconfigure traffic forwarding from Endpoint Agent to Sensor and trusted connection with Endpoint Agent.
- Upload a new certificate to Active Directory (if you are using Active Directory).

Delete all Endpoint Agent host isolation rules. The connection with isolated hosts is severed and you cannot manage them.

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 window of the program web interface, select the **Settings** section, **Certificates** subsection.
3. In the **Server certificate** section, 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 Anti Targeted Attack Platform. Reconfigure traffic forwarding from Endpoint Agent to Sensor and trusted connection with Endpoint Agent.

- Upload a new certificate to Active Directory (if you are using Active Directory).

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

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

To upload a TLS certificate of the Central Node server or Sensor 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 integration settings** 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 pinned certificate to secure connection** check box.

8. Click **Add a TLS certificate...**.

   This opens the **Adding TLS certificate** window.

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 is displayed, select a certificate file and click **Open**.

   - Paste the content of the certificate file to the **Paste TLS certificate data:** 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. Make sure the toggle switch in the upper right corner of the group of settings is in the **Under policy** position.

12. Click **OK**.

The TLS certificate of the Central Node server is downloaded 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 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 **Settings** section, **Certificates** subsection.

3. In the **Endpoint Agent certificates** section, 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 **Settings** section, **Certificates** subsection.
3. In the **Endpoint Agent certificates** section, 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 cryptographic 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 cryptographic 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 a manually prepared TLS certificate of Kaspersky Endpoint Agent using the web interface of Kaspersky Anti Targeted Attack Platform:

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 **Settings** section, **Certificates** subsection.
3. In the **Endpoint Agent certificates** section, 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 **Settings** section, **Certificates** subsection.

3. The **Endpoint Agent certificates** section displays a list of TLS certificate with the following details 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 **Settings** section, **Certificates** subsection.
3. The **Endpoint Agent certificates** section displays a list of TLS certificate with the following details 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 to 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 **Settings** section, **Endpoint Agent certificates** subsection.

   The **Endpoint Agent certificates** section displays a list of TLS certificates.
3. Select check boxes next to one or more TLS certificates that you want to delete.
4. Click **Delete**.

   This opens the action confirmation window.
5. 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 **Download**.

   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. Make sure the toggle switch in the upper right corner of the group of settings is in the **Under policy** position.

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 the Endpoint Agent component to the Sensor server

You can use the Sensor server as a proxy server for communication between the Endpoint Agent component and the Central Node to reduce the load on the Central Node. To do this, when connecting the application that acts as the Endpoint Agent component, on the side of that application, you need to specify the IP address of the Sensor server instead of the IP address of the Central Node server. Sensor must be installed on a different server than the Central Node.

When configuring the traffic redirection, keep in mind the following limitations:

- The maximum incoming traffic volume for the Sensor may not exceed 1 Gbps.
- The recommended channel bandwidth between Central Node and Sensor servers must be 15% of the SPAN port traffic.
- The maximum allowed packet loss between Sensor servers and the Central Node is 10% with a packet delay of up to 100 ms.

To use the Sensor as a proxy server, connect the Sensor to the Central Node.

Enabling traffic redirection from Kaspersky Endpoint Agent to the Sensor server

To enable the use of 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 with 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**.

   This opens a window with information about the current state of connection of the Sensor component to the Central Node component.
5. Click **Change**.
6. In the **Input Central Node IP address** window, enter the IP address of the server hosting the Central Node component.
7. Click **Ok**.

   This opens a window containing information on the Central Node component certificate.
8. Make sure that the displayed certificate matches the Central Node component certificate.
9. Click **Ok**.

   This opens a window with information about the current state of connection of the Sensor component to the Central Node component.
10. Click **Cancel**.

Using the Sensor component as a proxy server will be enabled 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 Central Node server, do the following in the web interface under the local administrator account:

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. Select the IP address of the server hosting the Sensor component, the request for authorization of which you want to confirm or reject.

3. Do one of the following:

   - If you want to authorize the selected server hosting the Sensor component, click **Accept**.
   - If you want to reject the authorization of the selected server hosting the Sensor component, click **Reject**.

The authorization request will be accepted or 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 your own TLS certificate in the administrator menu of the Sensor server

You can prepare your own TLS certificate and upload it to the Sensor server using SCP. 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 OpenSSL documentation.

To upload your own TLS certificate to the Sensor server using SCP, do the following in your computer's SCP interface (Linux is used in the 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 managing the administrator menu of the Sensor server that was set during installation.

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

To apply the uploaded TLS certificate on the Sensor server, 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 **Install from file**.
6. Press **ENTER**.

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 directory.

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

To configure 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 integration settings** 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 pinned certificate to secure connection** check box.

8. Click **Add a TLS certificate...**.

   This opens the **Adding TLS certificate** window.

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 is displayed, select a certificate file and click **Open**.
   - Paste the content of the certificate file to the **Paste TLS certificate data:** 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 **Add client certificate...**.

12. In the window that is displayed, select the **Secure with client certificate** check box.

13. Click **Download**.

    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 period (sec.):** field, enter the maximum response timeout of the Kaspersky Anti Targeted Attack Platform Central Node server in seconds.

17. In the **Send sync request to KATA server every (min.)** field, enter the period in minutes.

18. If you do not want Kaspersky Endpoint Agent to send information about repeated running of processes to the Kaspersky Anti Targeted Attack Platform server, select the **Apply TTL period for events transmission** check box. If the process is started after the next TTL period expires, Kaspersky Endpoint Agent does not consider this a repeated start of the process.

19. If you have set the "Apply TTL period for events transmission" check box, specify the time in the **TTL period (min.)** field.

20. Make sure the toggle switch in the upper right corner of the group of settings is in the **Under policy** position.

21. Click **OK**.

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

Getting started with the application

This section contains information about how to begin managing the application in the web interface, in the administrator menu, and in Technical Support Mode.

Getting started with the web interface for sizing management

The Kaspersky Anti Targeted Attack Platform web interface for sizing management 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.

In the web interface for sizing management, you can do the following:

- Manage the servers of the Central Node cluster.
- Configure servers hosting the Central Node component.

To get started in the web interface for sizing management:

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 into the browser's address bar.

   If you are using the fault-tolerant version of the program, you can enter the IP address of any server of the Central Node cluster or **the fully qualified domain name (FQDN) of the cluster**.

   To ensure uninterrupted access to the program web interface, you can configure the Round Robin function on the DNS server. To do this, log in to the web interface of the first healthy server of the Central Node cluster.

   An input window for account credentials of the Kaspersky Anti Targeted Attack Platform user opens.

2. Enter the administrator user name "admin" and the password that was specified during installation of the program.

3. Select the **Local administrator** check box.

4. Click **Log in**.

You can now start working in the web interface for sizing management.

For the fault-tolerant version of the program, the web interface displays the **Cluster** and **Server configuration** sections.

If you are using the non fault-tolerant version of the program, only the **Server configuration** section is displayed in the 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 application web interface with a local administrator account

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.

After installing Kaspersky Anti Targeted Attack Platform, you must configure the sizing settings of the application in the web interface for sizing management.

If the sizing settings of Kaspersky Anti Targeted Attack Platform are not configured, it is not possible to log in to the web interface with a local administrator account.

To get started with the application web interface with a local administrator account:

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 into the browser's address bar.

   If you are using the fault-tolerant version of the program, you can enter the IP address of any server of the Central Node cluster or **the fully qualified domain name (FQDN) of the cluster**.

   To ensure uninterrupted access to the program web interface, you can configure the Round Robin function on the DNS server. To do this, log in to the web interface of the first healthy server of the Central Node cluster.

   An input window for account credentials of the Kaspersky Anti Targeted Attack Platform user opens.

2. Enter 'Administrator' as the account name and 'Administrator' as the password.

   The 'Administrator' password is used by default. We strongly recommend changing the password for this account after logging in to the application web interface.

3. Select the **Local administrator** check box.

4. Click **Log in**.

   The **Dashboard** page of the program web interface opens.

You can start using the application with a local administrator account.

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 server management hosting the needed component:

1. Sign in to the management console of the server whose settings you want to change via the SSH protocol or through a terminal.

   The program component administrator menu is displayed.

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 application administrator menu.

Getting started with the program in Technical Support Mode

Any actions in Technical Support Mode that are not approved and/or not recommended by Technical Support staff are prohibited and are grounds for withdrawing technical support.

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 working with the Sandbox, Sensor or Central Node component 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 component.

   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. Confirm that you want to operate the program in Technical Support Mode. To do so, select **Yes** and press **ENTER**.

You can now start working in Technical Support Mode.

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 auditor**, **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 take steps to ensure the security of the servers. 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 lets you 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 tenants in the **Operation mode** section.

An account with the **Security auditor** role can view all sections of the web interface available to the local administrator and security personnel. A user with the **Security auditor** role can view data but cannot edit this data.

The **Senior security officer** and **Security officer** roles are intended for employees of your organization whose job description involves managing 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. Users with the **Senior security officer** role have access to all operations. The restrictions for users with the **Security officer** role are listed in the table below.

Access restrictions for program users with the **Security officer** role

Functional scope / Section of the web interface	Restrictions
Dashboard	Widgets of VIP group events are not available. It is not possible to use a link in the widget to go to the **Alerts** section.
Alerts	The following actions are not available: • Viewing alert details. • Marking the completion of VIP group alert processing. • Performing operations on multiple alerts. • Exporting the list of all alerts.
Threat Hunting	Events that are associated with hosts from VIP group alerts are not available.
Tasks	No access.
Prevention	No access.
Custom rules	Read access.
Storage	There is no access to objects that are placed in Storage as a result of tasks. Full access to objects that were manually downloaded by the user.
Endpoint Agents	Access to viewing tables of Kaspersky Endpoint Agent computers; restrictions on viewing details of tasks, policies, and network isolation.
Network isolation of hosts	No access.
Reports	No access.
Settings: IOC scanning schedule	Read access.
Settings: Endpoint Agents	Read access.
Settings: KPSN reputation database	No access.
Settings: Notification rules	No access to rules for sending notifications about alerts. Full access to rules for sending notifications about problems in program operation.
Settings: VIP status	Read access.
Custom rules: YARA	Access only to export rules.
Settings: TAA exclusions	Access to read and export.
Settings: Passwords for archives	No access.
Settings: License	Read access.

If you are using the distributed solution and multitenancy mode, access to tenants and the web interface of the SCN server can be allowed or denied for each account.

Creating an administrator account for the program web interface

The administrator account of the program web interface lets you 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 tenants in the **Operation mode** section.

To create a program web interface administrator account:

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Click **Add**.

   This opens the **New user** window.
4. To enable an account, turn on the **Status** toggle switch.

   By default, the account is enabled.

   > If a user account is enabled, the user is allowed to access the program web interface. If a user account is disabled, the user is prohibited from accessing the program web interface.
5. In the **Role** drop-down list, select **Administrator**.
6. Under **Authentication type**, select one of the following options:

   - **KATA user account**.

     In this case, to connect to the program web interface, the user must enter the user name and password that were configured when the account was created.
   - **Domain user account**.

     In this case, to connect to the program web interface, the user does not have to enter the user name and password; the user is authenticated with the domain account.

   > The **KATA user account** and **Domain user account** fields are available if Active Directory integration is configured.
7. If you selected **KATA user account**:

   a. 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).

b. 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.

c. In the **Confirm password** field, re-enter the user password that will be used to access the web interface.

8. If you selected **Domain user account**, in the **User name** field, enter the user's domain name.
9. Click **Add**.

This will create an administrator account for the program web interface.

If you are using the distributed solution and multitenancy mode, the administrator account of the PCN server web interface has access to the data of all organizations associated with that server.

Creating a user account for the program web interface

You can create user accounts with the **Senior security officer**, **Security officer**, and **Security auditor** roles.

To create a user account for the program web interface:

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Click **Add**.

   This opens the **New user** window.
4. If necessary, disable the user account using the **Status** toggle switch.

   By default, the account is enabled.

If a user account is enabled, the user is allowed to access the program web interface. If a user account is disabled, the user is prohibited from accessing the program web interface.

5. Under **Authentication type**, select one of the following options:

- **KATA user account**.

  In this case, to connect to the program web interface, the user must enter the user name and password that were configured when the account was created.

- **Domain user account**.

  In this case, to connect to the program web interface, the user does not have to enter the user name and password; the user is authenticated with the domain account.

  If you have selected the **Domain user account** authentication type, note that the user will not be able to log in to the program web interface with a different user account.

The **KATA user account** and **Domain user account** fields are available if Active Directory integration is configured.

6. In the **Role** drop-down list, select one of the following roles:

- **Senior security officer**
- **Security officer**
- **Security auditor**

7. If you selected **KATA user account**:

   a. 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).

   b. 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.

c. In the **Confirm password** field, re-enter the user password that will be used to access the web interface.

8. If you selected **Domain user account**, in the **User name** field, enter the user's domain name.
9. In the **Access** section, configure access rights:

   a. Turn on the **SCN web interface** toggle 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 **Tenants** setting title, select check boxes for one or more tenants to whose web interfaces you want to grant access.

   You can use the **Select all** and **Deselect all** links to select or unselect all tenants.

10. Click **Add**.

Configuring user account table display

You can show or hide columns and change the order of columns in the table of application web interface user accounts.

To configure the display of the application web interface user account table:

1. Log in to the web interface with the application administrator account.
2. In the window of the application web interface, select the **Settings** section, **Users** subsection.
3. In the heading part of the table, click  .

   This opens the **Customize table** window.
4. If you want to show a column in the table, select the check box next to the name of the parameter that you want displayed in the table.

   If you want to hide a parameter in the table, clear the check box.

   > At least one check box must be selected.
5. If you want to change the order of columns in the table, move the mouse cursor to the row with the relevant parameter, click  and move the row to its new place.

6. If you want to restore default table display settings, click **Default**.

7. Click **Apply**.

User account table display is configured.

Viewing the user account table

The event table is displayed in the **Settings** section, **Users** subsection of the program web interface window. You can sort events in the table by the **User name**, **Role**, **Tenants**, and **Status** columns.

The table contains the following information:

1. **User name** is the user name configured when creating the account.

2. **Authentication type** is the authentication type of the user. Possible values:

   - **KATA user account**.

     In this authentication type is selected, to connect to the program web interface, the user must enter the user name and password that were configured when the account was created.

   - **Domain user account**.

     If this authentication type is selected, to connect to the program web interface, the user does not have to enter the user name and password; the user is authenticated with the domain account.

3. **Role** is the role assigned to the user.

4. **Tenants** is a list of tenants to which the user has access.

   This column is displayed only in distributed solution and multitenancy mode.

5. **Status** is the status of the account. Can have the following values:

   - **Enabled**

     If a user account is enabled, the user is allowed to access the program web interface.

   - **Disabled**

     If a user account is disabled, the user is prohibited from accessing the program web interface.

Filtering user accounts

To filter or search for user accounts by required criteria:

1. Log in to the web interface with the program administrator account.

2. In the window of the program web interface, select the **Settings** section, **Users** subsection.

3. Depending on the filtering criterion, do the following:

- **By user name**

  a. Click the **User name** link to open the filtering menu.

  b. In the drop-down list, select one of the following filtering operators:

  - **Contains**
  - **Does not contain**

  c. In the text box, type the user name or a sequence of characters from the user name.

  d. Click **Apply**.

- **By authentication type**

  a. Click the **Authentication type** link to open the filtering menu.

  b. Select the check box next to the account that you want to include in filtering criteria:

  - **KATA user account**.
  - **Domain user account**.

  c. Click **Apply**.

- **By role**

  a. Click the **Role** link to open the filtering menu.

  b. Select check boxes corresponding to roles that you want to add to filter criteria.

  - **Administrator**
  - **Senior security officer**
  - **Security officer**
  - **Security auditor**

  You can select multiple check boxes.

  c. Click **Apply**.

- **By names of tenants that the user has access to**

  a. Click the **Tenants** link to open the filtering menu.

  b. Select check boxes corresponding to tenants that you want to add to filter criteria.
  You can select multiple check boxes.

  c. Click **Apply**.

- **By status**

  a. Click **Status** to expand the filter settings list.

  b. Select one of the following options:

  - **All**
  - **Enabled**
  - **Disabled**

The table displays accounts that correspond to configured filter criteria.

You can use multiple filters at the same time.

Clearing the account filter

To clear the user account filter by one or more filtering conditions:

1. Log in to the web interface with the application administrator account.
2. In the window of the application web interface, select the **Settings** section, **Users** subsection.
3. Click to the right of the header of the user account 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 displays only user accounts that match the specified criteria.

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 to data of PCN and SCN servers as well as tenants to which those servers belong.

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 **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 **Status** 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 **Disabled** if you want to grant the user access only to the web interface of this PCN server.
5. To the right of the **Tenants** setting name, select or clear check boxes of one or more tenants for which you want to change the access rights of server web interfaces.

   You can use the **Select all** and **Deselect all** links to select or unselect all tenants.
6. Click **Save**.

The access rights of the account are changed.

Enabling or disabling a user account

If you are using the distributed solution and multitenancy mode, follow these steps in the web interface of the PCN. User account status management is not available in web interface of an SCN.

To enable or disable a user account:

1. Log in to the web interface with the application administrator account.
2. In the window of the application web interface, select the **Settings** section, **Users** subsection.
3. In the list of accounts, select the user account that you want to enable or disable.
4. In the **Status** column, do one of the following:

   - Set the toggle switch next to the name of a user account to **Enabled** if you want to enable the user account.
   - Set the toggle switch next to the name of a user account if you want to **Disabled** the user account.

The action confirmation window is displayed.

5. Click **Yes**.

The state of the account is modified.

The Administrator account cannot be disabled.

Changing the password of a program administrator or user account

Only users with the **KATA user account** authentication type can change the password of their 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 **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

Only users with the **KATA user account** authentication type can change the password of their user account.

To change the password of your user account:

1. Sign in to the web interface with your account.
2. In the lower part of the program web interface window, click the link with the name of your account to expand the action list.
3. Select the **Change password** action.

   This opens the **Change password** window.
4. In the **Old password** field, enter the current password for the program web interface.
5. In the **New password** field, enter a new password for the program web interface.

   The password must satisfy the following requirements:

   - Must not be the same as the user name.
   - Must not contain dictionary words, popular combinations of letters, or examples of a keyboard layout (for example, Qwerty or passw0rd).
   - Must contain at least 8 characters.
   - Must contain at least three types of characters:
     - Uppercase character (A–Z).
     - Lowercase character (a–z).
     - Number.
     - Special character.
6. In the **Confirm password** field, enter the new password again.
7. Click **Change password**.

This will change your user account password for accessing the program web interface.

Authentication using domain accounts

If authentication using domain accounts is configured, users do not have to enter Kaspersky Anti Targeted Attack Platform account credentials to connect to the program web interface.

To enable authentication using domain accounts:

1. Configure integration with Active Directory.

   To set up the Active Directory integration, you must create a keytab file containing the service principal name (hereinafter also "SPN") for the Central Node server on which you want to set up the integration.

2. Select the **Domain user account** authentication type for the user when creating the account.

Creating a keytab file

You can create one user account to authenticate at multiple Central Node servers. Service principal name (SPN)To do so, you must create a keytab file that contains *service principal names (hereinafter also SPN)* for each of these servers. When you create the keytab file, you must use an attribute to generate a *salt* (hash function input modifier).

> The generated salt must be saved in any convenient way for adding more SPNs to the keytab file in the future.

You can also create a separate Active Directory user account for each Central Node server for which you want to set up Kerberos authentication.

To create a keytab file using one user account:

1. On the domain controller, in the **Active Directory Users and Computers** snap-in, create a user account (for example, with `control-user` as its name).

2. If you want to use the AES256-SHA1 encryption algorithm, in the **Active Directory Users and Computers** snap-in:

   a. Open the properties of the user account that you have created.

   b. On the **Account** tab, select the **This account supports Kerberos AES 256 bit encryption** check box.

3. Use the ktpass utility to create a keytab file for the `control-user` user. To do so, run the following command on the command line:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<fully qualified domain name (FQDN) of the Central Node server>@<realm name of the Active Directory domain in uppercase> -mapuser control-user@<realm name of the Active Directory domain in uppercase> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out <path to the file>\<file name>.keytab
   ```

   The utility requests the `control-user` password when executing the command.

   The SPN of the selected server is added to the created keytab file. The generated salt is displayed on screen: `Hashing password with salt "<hash value>".`

4. Add an SPN record for each subsequent Central Node server to the keytab file. To do so, run the following command:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<fully qualified domain name (FQDN) of the Central Node server>@<realm name of the Active Directory domain in uppercase> -mapuser control-user@<realm name of the Active Directory domain in uppercase> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <path and name of the previously created file>.keytab -out <path and new name>.keytab -setupn -setpass -rawsalt "<hash value of the salt obtained when creating the keytab file at step 3>"
   ```

   The utility requests the `control-user` password when executing the command.

The keytab file is created. This file contains all added SPNs of selected servers.

Example:

For example, you need to create a keytab file containing SPN names of 3 servers: `control-01.test.local`, `secondary-01.test.local`, and `secondary-02.test.local`.

To create a `filename1.keytab` file containing the SPN of the server in C:\keytabs\, run the command:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * +dumpsalt -out C:\keytabs\filename1.keytab
```

Let's say you got `"TEST.LOCALHTTPcontrol-01.test.local"` as the salt.

To add another SPN, run the following command:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

To add a third SPN:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab -setupn -setpass -rawsalt "TEST.LOCALHTTPcontrol-01.test.local"
```

This creates a `filename3.keytab` file containing all three added SPNs.

To create a keytab file using a separate account for each Central Node server:

1. On the domain controller server, in the **Active Directory Users and Computers** snap-in, create a separate user account for each server (for example, `control-user`, `secondary1-user`, `secondary2-user`, etc).

2. If you want to use the AES256-SHA1 encryption algorithm, in the **Active Directory Users and Computers** snap-in:

   a. Open the properties of the user account that you have created.

   b. On the **Account** tab, select the **This account supports Kerberos AES 256 bit encryption** check box.

3. Use the ktpass utility to create a keytab file for the `control-user` user. To do so, run the following command on the command line:

   ```
   C:\Windows\system32\ktpass.exe -princ HTTP/<fully qualified domain name (FQDN) of the Central Node server>@<realm name of the Active Directory domain in uppercase> -mapuser control-user@<realm name of the Active Directory domain in uppercase> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out <path to the file>\<file name>.keytab
   ```

   The utility requests the `control-user` password when executing the command.

   The SPN of the selected server is added to the created keytab file.

4. Add an SPN record for each subsequent Central Node server to the keytab file. To do so, run the following command:

```
C:\Windows\system32\ktpass.exe -princ HTTP/<fully qualified domain name (FQDN) of the Central Node server>@<realm name of the Active Directory domain in uppercase> -mapuser secondary1-user@<realm name of the Active Directory domain in uppercase> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in <path and name of the previously created file>.keytab -out <path and new name>.keytab
```

The utility requests the `secondary1-user` password when executing the command.

The keytab file is created. This file contains all added SPNs of selected servers.

Example:

For example, you need to create a keytab file containing SPN names of 3 servers: `control-01.test.local`, `secondary-01.test.local`, and `secondary-02.test.local`.

To create a `filename1.keytab` file containing the SPN of the server in C:\keytabs\, run the command:

```
C:\Windows\system32\ktpass.exe -princ HTTP/control-01.test.local@TEST.LOCAL -mapuser control-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -out C:\keytabs\filename1.keytab
```

To add another SPN, run the following command:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-01.test.local@TEST.LOCAL -mapuser secondary1-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename1.keytab -out C:\keytabs\filename2.keytab
```

To add a third SPN:

```
C:\Windows\system32\ktpass.exe -princ HTTP/secondary-02.test.local@TEST.LOCAL -mapuser secondary2-user@TEST.LOCAL -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass * -in C:\keytabs\filename2.keytab -out C:\keytabs\filename3.keytab
```

This creates a `filename3.keytab` file containing all three added SPNs.

Configuring integration with Active Directory

To configure integration with Active Directory:

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Go to the **Active Directory integration** tab.
4. Select the **Integration** check box if you want to enable integration with Active Directory.
5. Click **Browse** to upload the keytab file.
6. Select the keytab file and click **Open**.

After you upload the file, the following fields are displayed:

- **Keytab file status**. Possible values:
  - **File contains SPN for this server** means the uploaded keytab file contains the SPN for that Kaspersky Anti Targeted Attack Platform server.
  - **No SPN for this server** means the uploaded keytab file does not contain the SPN for that Kaspersky Anti Targeted Attack Platform server.
- **The file contains** is the list of SPNs that the file contains.

7. Click **Apply**.

Integration with Active Directory is configured.

In distributed solution and multitenancy mode, Active Directory integration settings configured on the PCN server are **not** applied to SCN servers connected to that PCN server. If you want to set up Active Directory integration on individual SCN servers, you must complete the steps above on each of the selected SCN servers.

Disabling integration with Active Directory

When integration with Active Directory is disabled, user authentication with domain accounts is not available.

To disable integration with Active Directory:

1. Log in to the web interface with the program administrator account.
2. In the window of the program web interface, select the **Settings** section, **Users** subsection.
3. Go to the **Active Directory integration** tab.
4. Clear the **Integration** check box.
5. Click **Apply**.

Integration with Active Directory is disabled. The uploaded keytab file is permanently deleted.

In distributed solution and multitenancy mode, Active Directory integration settings configured on the PCN server are **not** applied to SCN servers connected to that PCN server. If you want to disable Active Directory integration on individual SCN servers, you must complete the steps above on each of the selected SCN servers.

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.

Personal information of the user is not collected, processed, or stored. For information about data that Kaspersky Anti Targeted Attack Platform sends to Kaspersky Security Network, refer to the KSN Statement.

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.

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 the distributed solution and multitenancy mode, participation in KSN is configured 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 the participation in Kaspersky Security Network:

1. Log in to the program web interface with the administrator account.
2. Select the **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 **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 clicking **Browse**.
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 KPSN reputation database:

1. Log in to the program web interface with the administrator account.
2. Select the **Settings** section, **KPSN reputation database** subsection.
3. In the **Host** field, specify the IP address of the KPSN server on which the local reputation database of KPSN is stored.
4. Click **Browse** 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 **Browse** 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 alert details to the local reputation database of KPSN:

1. Log in to the program web interface under the senior security officer account.
2. Select the **Settings** section, **KPSN reputation database** subsection.

3. Do one of the following:

   - Turn on the **Assign the "Untrusted" status to objects** 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 objects** 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 **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.

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.

To get started with the web interface of the Sandbox application:

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.

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

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 upgrade packages* (or upgrade packages). Upgrade packages consist of one or more files containing records to identify threats that were detected since the previous upgrade package was released. We recommend that you regularly receive upgrade 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:

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 update server (secure connection)**.

     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 selected **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 updating the Sandbox component databases:

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 the proxy server connection for updating Sandbox component databases:

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. A request for connection to the Sandbox component is created in the program web interface.
2. The Sandbox web interface shows connection requests.

   You can accept or reject a request.

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 Central Node servers:

1. Select the **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:

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:

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Management interface** settings group from the **Interface** drop-down list, select a network interface, which you want to use as a management interface.
3. In the **IP** field, enter the IP address that you want to assign to this network interface if no IP address is assigned.
4. In the **Mask** field, enter the network mask in which you want to use this network interface.
5. Click **Apply** in the lower part of the window.

Configuring settings of a network interface used for Internet access of processed objects

Objects processed by the Sandbox component may attempt activities on the Internet via the network interface used for Internet access of processed objects. The Sandbox component can analyze the behavior of these objects.

If you block Internet access, the Sandbox component cannot analyze the behavior of objects on the Internet, and will therefore only analyze the behavior of objects without Internet access.

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

If the security policy of your organization denies access to the Internet from computers of local network users, and you have configured the Sandbox network interface for Internet access of processed objects, there is a risk of the following scenario:

A hacker can attach a malicious program to a random file and initiate a Sandbox scan of this file from the computer of a local network user. This file will be taken over outside the local network through the network interface used for Internet access of processed objects in the course of scanning the file by the Sandbox component.

Unavailability of the Sandbox network interface for Internet access of processed objects eliminates any risk of such data transfer but compromises the quality of alerts.

To configure the network interface used for Internet access of processed objects:

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Internet interface** settings group from the **Interface** list, select a network interface that you want to use for Internet access of processed objects.

   The management network interface that you configured previously cannot be selected from this list of network interfaces.

3. In the **IP** field, enter the IP address that you want to assign to this network interface.
4. In the **Mask** field, enter the network mask in which you want to use this network interface.
5. In the **Default gateway** field, enter the gateway address of the network in which you want to use this network interface.
6. Click **Apply** in the lower part of the window.

Adding, changing and removing static network routes

You can configure static network routes during installation of the Sandbox component.

You can also add, remove or change static network routes from the Sandbox web interface.

To add a static network route:

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Static Routes** settings group, click the **Add** button.

   A line with empty fields will be added in the list of static network routes.

3. In the **IP** field, enter the IP address of the server for which you want to configure a static network route.
4. In the **Mask** field, enter the subnet mask.
5. In the **Gateway** field, enter the IP address of the gateway.
6. From the **Interface** list, select a network interface for which you want to add a static network route.
7. Click ✓.
8. Click **Apply** in the lower part of the window.

To remove a static network route, proceed as follows:

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Static Routes** settings group in the line containing the static network route that you want to remove, click the 🗑 button.
3. Click **Apply** in the lower part of the window.

To modify a static network route:

1. Select the **Network Interfaces** section in the window of the Sandbox web interface.
2. In the **Static Routes** settings group in the line containing the static network route that you want to change, click the button.

   The static network route line will become editable. You can change one or more parameters of a static network route.
3. In the **IP** field, change the IP address of the server for which you want to configure a static network route.
4. In the **Mask** field, change the subnet mask.
5. In the **Gateway** field, change the IP address of the gateway.
6. From the **Interface** list, select the network interface for which you are editing the network route.
7. Click .
8. Click **Apply** in the lower part of the window.

Updating the Sandbox system

Kaspersky 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 using the web interface:

1. Select the **System Upgrade** section in the window of the Sandbox web interface.

   The current version of the Sandbox component is displayed to the right of the **Current version** setting label.
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 the date and time on the server hosting the Sandbox component:

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 ISO images of the following operating systems: Windows XP SP3, Windows 7 64-bit, Windows 10 64-bit, and CentOS 7.8, Astra Linux 1.7, as well as software required for the operation of the Sandbox component. You do not have to activate these operating systems and programs. The images already include a 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**.

   When installing virtual machines with the Windows XP SP3, Windows 7, Windows 10 and Astra Linux 1.7 operating systems, the **EULA** window opens, which contains the contents of the following license agreements:

   - For Windows XP SP3, Windows 7, and Windows 10 operating systems:
     - 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.

- For the Astra Linux 1.7 operating system:
  - THE END USER LICENSE AGREEMENT FOR ASTRA LINUX SOFTWARE is included in Kaspersky Anti Targeted Attack Platform.

When installing a virtual machine that runs the CentOS 7.8 operating system, the **EULA** window does not appear because you do not need to accept the terms of the end user license agreement to use this operating system.

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 by 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:

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 programs 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 logical 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:

1. In the Sandbox web interface window, select the **Administration** section.
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 settings of a Sandbox system:

1. In the Sandbox web interface window, select the **Administration** section.
2. In the **Settings** settings group, click the **Export** button.

   This opens the **Warning** window containing a warning on specifics of exporting the system parameters.

   The Sandbox system parameters are dependent on hardware and software parameters of the server, on which the Sandbox component is installed. The Sandbox system exported parameters are intended to be imported to the same or another server strictly identical in configuration. Any attempt to restore the configuration of the Sandbox system with parameter values saved to another Sandbox system may disrupt the Sandbox system.
3. Click **Save**.

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 Sandbox settings:

1. In the Sandbox web interface window, select the **Administration** section.
2. In the **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 **Restore**.

   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:

1. In the Sandbox web interface window, select the **Administration** section.
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 power off the Sandbox server:

1. In the Sandbox web interface window, select the **Administration** section.
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:

1. In the Sandbox web interface window, select the **Administration** section.
2. The **Change password** 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 **Change password**.

   The Sandbox administrator account password will be changed.

For the administrator: Getting started in the program web interface

The intended audience of this section are personnel who install and administer Kaspersky Anti Targeted Attack Platform and manage PCN and SCN servers and tenants 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/Security auditor**.

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 contains the following sections:

- **Dashboard**. Contains Kaspersky Anti Targeted Attack Platform Monitoring data.
- **Operation mode**. Contains information about PCN and SCN servers and about tenants in distributed solution and multitenancy mode.
- **Endpoint Agents**. Contains information about connected computers with Kaspersky Endpoint Agent program and their settings.
- **Reports**: **Activity log**. Contains information about the logging settings for user activity in the program web interface.
- **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.

Users with the **Security auditor** role can also view these sections of the program web interface.

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.

A *layout* is the appearance of the workspace of the program web interface window in the **Dashboard** section. You can add, delete, and move widgets in 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 distributed solution and multitenancy mode, the section displays information about the tenant and server that you chose.

Selecting a tenant and a server to manage in the Dashboard section

If you are using the distributed solution and multitenancy mode, before using the **Dashboard** section, you must select the tenant and server whose data you want to view.

*To select a tenant and server for which you want to display data 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 tenant and server from the list.

Data for the selected server is displayed. If you want to select a different tenant and server, repeat the steps to select a tenant and server.

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, turn on the toggle switch next to the name of this widget.
   - If you want to add the **Sandbox processing time** widget, turn on the toggle switch 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 is 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 the upper part of the widget to drag and drop the widget to a different place in the layout.
6. Click **Save**.

The current layout is 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 is removed from the workspace of the program web interface window.
5. Click **Save**.

The widget is 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 is saved to the hard drive of your computer in the downloads folder of the browser.
6. Click **Close**.

Configuring the data display period in widgets

You can configure the display of data in widgets for the following periods:

- **Day**
- **Week**
- **Month**

To configure the display of data in widgets for a day (from 00:00 a.m. to 11:59 p.m.):

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 display data in 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 display data in the widget.

All widgets on the **Dashboard** page display data for the period you selected.

To display data display in widgets for a month (calendar month):

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 display data in 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 component to the server with the Central Node component, and track data processing errors.

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 legend for colors used in the widget itself.

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 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 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 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 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 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 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 monitor 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 the widget displays the legend for colors used in 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 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 elapsed from the moment data is sent to one or multiple Sandbox component servers (including the time spent in the queue before getting sent) to the moment when the Sandbox processing results are displayed in the web interface of Kaspersky Anti Targeted Attack Platform for the selected period.

Example:
If **Month** is configured as the period of data display in widgets, the **Sandbox processing time** widget displays orange-colored bars 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.

Users with the **Local administrator**, **Administrator**, or **Security auditor** roles can gain access to 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**, **Security officer**, or **Security auditor** roles can gain access to 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 gain access to information about the working condition of that SCN server for tenants to whose data the user has access.
- If you are using the distributed solution and multitenancy mode, and the user is managing the PCN server, the user can gain access to information about the working condition of the PCN server and all SCN servers connected to that server, for tenants to whose data the user has access.

For details about the working condition of program modules and components,

click **View details** to open the **System health** window.

In the **System health** window, one of the following icons is displayed depending on the working condition of the program modules and components:

- OK if the modules and components of the program are working normally.
- An icon with the number of problems (for example, 1) if problems are found that the administrator is recommended to pay attention to. 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:

- **Component health** contains information on the operational status of program modules and components, Quarantine, and database 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**—Status 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.
- **Connection with servers**—Status 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.
- Monitor the disk space usage 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.

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 **Settings** section, **Date and time** subsection.
2. In the **Time zone** drop-down list, select the time zone of the physical location of the server with the Central Node component.

   You can specify the country and time zone by selecting the relevant region on the map under the drop-down lists.
3. In the **NTP servers** section:
   - If you want to add a new NTP server:
     a. Click **Add**.
     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.
4. Click **Apply**.

The date and time of the server will be configured.

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 the connection of Central Node, PCN, and SCN to Sandbox.
- Reconfigure traffic forwarding from Endpoint Agent to Sensor and trusted connection with Endpoint Agent.
- Upload a new certificate to Active Directory (if you are using 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 a Central Node server:

1. Sign in to the Kaspersky Anti Targeted Attack Platform web interface with the administrator credentials.
2. In the window of the program web interface, select the **Settings** section, **Certificates** subsection.
3. In the **Server certificate** section, click **Generate**.

   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 window of the program web interface, select the **Settings** section, **Certificates** subsection.
3. In the **Server certificate** section, 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.

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 of the server:

1. In the window of the program web interface, select the **Settings** section, **Certificates** subsection.
2. In the **Server certificate** section, click **Download**.

   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 **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 server 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:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. In the **DNS settings** group, enter the IP addresses of the DNS servers in the **Primary and Secondary DNS servers** field.
3. 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 network interface:

1. In the window of the program web interface, select the **Settings** section, **Network settings** subsection.
2. Select the network interface whose settings you want to configure.

   This opens the **Edit network interface** window.
3. In the **State** settings group, select one of the following options:
   - **Disabled**.
   - **Enabled, using DHCP server** if you want the settings received from the DHCP server to be used for the network interface.
   - **Enabled, manual configuration** if you want the manually configured network interface to be used.
4. If you selected **Enabled, manual configuration**, specify values for the following parameters:
   a. In the **IP** field, specify the IP address of the network interface.
   b. In the **Subnet mask** field, specify the subnet mask of the network interface.
   c. In the **Gateway** text box, enter the IP address of the gateway.
5. 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 **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:

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Proxy server** settings group, set the toggle switch to **Enabled**.
3. In the **Host** field, specify the URL of the proxy server.
4. In the **Port** field, specify the port for connecting to the proxy server.
5. In the **User name** field, specify the user name for authentication on the proxy server.
6. In the **Password** field, specify the password for authentication on the proxy server.
7. If you do not want to use a proxy server when connecting to local addresses, select the **Bypass proxy server for local addresses** check box.
8. Click **Apply**.

The proxy server connection settings will be configured.

Configuring the mail server connection

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 program can send notifications about alerts and system performance. To do so, you must configure the settings of the server used for sending notifications.

To configure the server for sending notifications:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Mail configuration** tab.
3. In the **Host** field, specify the IP address of the mail server.
4. In the **Port** field, specify the port for connecting to the mail server.
5. In the **Email from** field, specify the email address from which the notifications will be sent.
6. If you want to enable authentication on the mail server, select the **Use SMTP authentication of message recipients** check box.
7. In the **User name** field, specify the user name for authentication on the server used for sending notifications.
8. In the **Password** field, specify the password for authentication on the server used for sending notifications.
9. If you want to use TLS encryption when sending notifications, select the **Use TLS encryption** check box.
10. 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.

11. Click **Apply**.

The settings of the server used for sending notifications will be configured.

Selecting operating systems to use when scanning objects in Sandbox

> 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 select a set of operating systems that will be used to generate tasks for scanning objects using the Sandbox component. On the Sandbox server, you must install virtual machines with operating systems that match the configured set.

To select the set of operating systems:

1. Select the **Sandbox servers** section in the window of the program web interface.
2. Go to the **Settings** tab.

3. Under **OS set**, select one of the following options:

   - Windows XP, Windows 7, Windows 10.
   - CentOS 7.8, Windows XP, Windows 7, Windows 10.
   - Astra Linux 1.7, Windows XP, Windows 7, Windows 10.

   Kaspersky Anti Targeted Attack Platform will create tasks for scanning objects in Sandbox in accordance with the selected set.

If the set of operating systems installed on the Sandbox server does not match the set selected on the Central Node server, objects are not sent to be scanned by that Sandbox server. If multiple Sandbox servers are connected to the Central Node server, the program sends objects to those Sandbox servers whose installed operating systems match the set selected on Central Node.

You can change the set of operating systems in the course of using the program. In this case, you need to make sure that the configuration of the Sandbox server satisfies hardware requirements.

In distributed solution and multitenancy mode, the settings of the operating system set configured on the PCN server are not applied to SCN servers connected to that PCN server. You can select the set of operating systems for each PCN and SCN server individually.

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 standalone 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.

Viewing the table of servers with the Sensor component

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.

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.

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 row 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 **Select CPU** 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 over 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.

If you have deployed the Central Node and Sensor components as a cluster, you can configure fault-tolerant integration with the mail server.

To configure fault-tolerant integration with the mail server:

1. Configure Round Robin on the DNS server for the domain name corresponding to the Central Node cluster.
2. Specify this domain name in the mail server settings.

   Integration with the mail server will be configured based on the domain name. The mail server will communicate with a random server in the cluster. If this server fails, the mail server will communicate with another healthy server in the cluster.

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 the mail server over 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** settings group, 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** settings group, 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. 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.

When a standalone proxy server is used, Kaspersky Anti Targeted Attack Platform does not provide encryption of ICAP traffic or authentication of ICAP clients by default. The program 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 ICAP:

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.

If you have deployed the Central Node and Sensor components as a cluster, you can configure fault-tolerant integration with a proxy server.

To configure the fault-tolerant integration with the proxy server:

1. Configure Round Robin on the DNS server for the domain name corresponding to the Central Node cluster.
2. Specify this domain name in the proxy server settings.

   Integration with the proxy server will be configured based on the domain name. The proxy server will communicate with a random server in the cluster. If this server fails, the proxy server will communicate with another healthy server in the cluster.

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 over 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.

    The mail server must support Basic Authentication.
11. In the **TLS certificate** drop-down list, select one of the following options:

    - **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.

If you have deployed the Central Node and Sensor components as a cluster, you can configure fault-tolerant integration with the mail server.

To configure fault-tolerant integration with the mail server:

1. Configure Round Robin on the DNS server for the domain name corresponding to the Central Node cluster.
2. Specify this domain name in the mail server settings.

   Integration with the mail server will be configured based on the domain name. The mail server will communicate with a random server in the cluster. If this server fails, the mail server will communicate with another healthy server in the cluster.

Managing the cluster

You can view the table of cluster servers, add servers to the cluster, decommission servers, and enable or disable the cluster. if necessary, you can increase the disk space on the storage server.

Viewing the table of servers of the cluster

The table of cluster servers is displayed in the **Cluster** section of the application web interface.

The table contains the following information:

- **Server type**—server type depending on its role in the cluster.

  The following values can be displayed:

  - **Storage**.
  - **Processing**.

- **Status**—server status.

The following values can be displayed:

- **Connected**.
- **Not connected**.

- **Host name**—server name.
- **IP**— IP address of the server.
- **RAM**—RAM load level of the server.
- **CPU**—CPU load level of the server.
- **Action**—Actions that you can perform with the server.
  The following action is available: **Delete**.

Adding a server to a cluster

To add a server to the cluster, you need to start the installation of Kaspersky Anti Targeted Attack Platform on this server and follow the steps to install the components. The added server is displayed in the cluster server list.

Increasing the disk space on the storage server

You can increase the disk space on an operational storage server by installing an additional disk.

> To increase the disk space of the storage server by means of an additional disk, you need to contact Technical Support.

The server is configured in Technical Support Mode.

Decommissioning servers

> To decommission an operational server, you need to contact Technical Support.

If a server fails, you can decommission it on your own.

To decommission an inoperable processing server:

1. Add a new processing server to the cluster.
2. Remove the server from the cluster.
3. Configure the sizing of the application for the new configuration.

The processing server will be decommissioned.

To decommission an inoperable storage server:

1. Add a new storage server to the cluster.
2. Contact Technical Support to remove the inoperable server from the cluster.

   The storage server will be decommissioned.

Removing a server from a cluster

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.

A removed server cannot be restored. Make sure that the selected server is not operational.

To remove a server from the cluster:

1. In the window of the application web interface, select the **Cluster** section.
2. In the **Action** column, click the **Delete** link opposite the server that you want to remove.
3. Click **Proceed**.

   The removal process will start. Removal may take about a day. Information about the removed server will not be displayed in the table of servers.

After removing the server, you can reconfigure the servers in the cluster or add a server with the same role to maintain the same level of application performance.

Starting up and shutting down the cluster

To shut down or start the cluster, we recommend contacting Technical Support. Do not shut down or start the cluster if you encounter problems with application health.

If you want to power off the healthy servers in the cluster, you must first shut down the cluster to avoid data loss.

To shut down a cluster:

1. In the application web interface, go to the **Cluster** section.
2. Click the **Shut down** button.

   The main components of the application are stopped. You can now power off the cluster servers.

To start up the cluster servers:

1. Disconnect power to the servers if it has not been previously disconnected.
2. Power on the storage server.
3. Power up the remaining servers.

   The cluster servers will start up.

It takes approximately 90 minutes for all servers in the cluster to start up. The application web interface becomes available before all cluster servers are started. However, for users with the **Senior security officer**, **Security officer**, **Security auditor** roles, the application web interface does not display the application menu, and users with the **Administrator** can manage only the **Server configuration** section.

We strongly discourage managing the sizing settings of the application until all the servers in the cluster are up and running.

When all of the servers in the cluster are up and running, the application web interface menu is displayed normally.

Notifications about the maximum allowed CPU and RAM load for the Central Node and Sensor servers

Maintaining a high load on the CPU and RAM of the Central Node and Sensor servers may prevent application components from working.

You can configure the maximum CPU and RAM usage on Central Node and Sensor servers; if these limits are exceeded, in the upper part of the **Dashboard** section of the application web interface for users with the **Senior security officer**, **Security officer**, and **Administrator** roles, a yellow warning box is displayed. You can also configure notifications to be sent to one or more email addresses and an SNMP protocol connection for sending information about the CPU and RAM load to external systems that support this protocol.

If you have deployed the Central Node and Sensor components as a cluster, warnings are displayed separately for each server in the cluster.

Users with the **Senior security officer** or **Security officer** role can also create rules for sending notifications. In this case, sending notifications correctly requires configuring maximum allowed load values for the CPU and RAM of servers, as well as notification settings on the server.

In existing rules for sending notifications about application components, the CPU load and RAM load notifications are enabled automatically if the **All** check box is selected under **Components** when the rule is created.

Configuring the maximum allowable CPU and RAM load of the Central Node and Sensor servers

In the distributed solution and multitenancy mode, you need to set the maximum allowed load values for the CPU and RAM load of each Central Node server from which you want to receive notifications. If you use a Central Node cluster, you can configure these settings on any cluster server.

To configure the maximum allowed load on the CPU and RAM of the Central Node and Sensor servers:

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. Under **Monitoring**:
   - In the **Warning of CPU usage above N % for M minutes** field, enter the maximum allowed CPU usage and time period for which the maximum load can be maintained.

     By default, the maximum CPU load is 95% for 5 minutes.
   - In the **Warning of RAM usage above N % for M minutes** field, enter the maximum allowed RAM usage and time period for which the maximum usage can be maintained.

     By default, the maximum RAM usage is 95% for 5 minutes.
3. Click **Apply**.

The maximum allowed load of server CPU and RAM will be configured. If one of the values is exceeded on the Central Node and/or Sensor server, in the upper part of the **Dashboard** section of the program web interface for users with **Senior security officer**, **Security officer**, **Administrator**, or **Local administrator** role, a yellow warning box is displayed.

Configuring the SNMP protocol connection

You can send information about the CPU and RAM load on Central Node and Sensor servers to external systems that support the SNMP protocol. To do so, you must configure the connection for the protocol.

If the Central Node component is deployed as a cluster, data about the CPU and RAM load of each server in the cluster is sent to external systems.

To configure the SNMP protocol connection on the Central Node server:

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. Under **SNMP**, select the **Use SNMP** check box.
3. In the **Protocol version** field, select a protocol version:
   - **v2c**.
   - **v3**.

4. If you selected the **v2c** protocol version, in the **Community string** field, enter the password that will be used for connecting to Kaspersky Anti Targeted Attack Platform.

5. If you selected **v3**:

   a. In the **Authentication protocol** field, select one of the following options for checking the accuracy and integrity of data sent to the external system:

   - **MD5**.
   - **SHA256**.

   b. In the **User name** field, enter the user name.

   c. In the **Password** field, enter the password for authentication.

   > User name and password configured in the **User name** and **Password** fields must match the user name and password configured when creating the account in the external system. If the credentials do not match, the connection cannot be established.

   d. In the **Privacy protocol** field, select an encryption type:

   - **DES**.
   - **AES**.

   e. In the **Password** field, enter the encryption password.

   > The password configured in this field must match the password configured in the external system.

Protocol connection on the Central Node server is configured. If the request for data is successfully processed, the server of the external system displays information about CPU and RAM load of the Central Node server.

To configure the SNMP protocol connection on the Sensor server:

1. Enter the management console of the Sensor server 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. Follow steps 2 through 5 of the instructions above.

Protocol connection on the Sensor server is configured. If the request is successfully processed, the server of the external system displays information about CPU and RAM load of the Sensor server.

> In distributed solution and multitenancy mode, SNMP connection settings for each PCN, SCN, and Sensor server must be configured separately.

Description of MIB objects of Kaspersky Anti Targeted Attack Platform

The tables below provide information about MIB objects of Kaspersky Anti Targeted Attack Platform.

Information about hard drive, CPU, and RAM load of Central Node and Sensor servers

Information about hard drive, CPU, and RAM load of Central Node and Sensor servers

Symbolic name	Description	Object identifier (OID)
`dskTotal`	Total size of the disk or partition, KB.	1.3.6.1.4.1.2021.9.1.6
`dskAvail`	Available space on the disk, KB.	1.3.6.1.4.1.2021.9.1.7
`dskUsed`	Used space on the disk, KB.	1.3.6.1.4.1.2021.9.1.8
`dskPercent`	Percentage of space used on disk, %.	1.3.6.1.4.1.2021.9.1.9
`laLoad`	System load average for 1, 5 and 15 minutes.	1.3.6.1.4.1.2021.10.1.3
`memTotalReal`	Total RAM size, KB.	1.3.6.1.4.1.2021.4.5
`memAvailReal`	Total RAM used, KB.	1.3.6.1.4.1.2021.4.6
`memTotalFree`	Total RAM free, KB.	1.3.6.1.4.1.2021.4.11

Managing Kaspersky Endpoint Agent host information

Kaspersky Endpoint Agent is installed on individual computers (hereinafter also referred to as "hosts") in the IT infrastructure of the organization. The program continuously monitors processes running on those hosts, active network connections, and files that are being modified.

Users with the **Senior security officer**, **Security officer**, **Security auditor**, **Local administrator**, or **Administrator** role 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 tenants to whose data the user has access. If you are using the distributed solution and multitenancy mode, the web interface of the PCN server displays the list of hosts with Kaspersky Endpoint Agent program 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 tenants to whose data they have 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 tenants to whose data the user has 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 staff 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, and other resources) and inform you about the scope of data obtained for debugging purposes. The retrieved diagnostic information 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 this manual 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 a tenant to manage in the Endpoint Agents section

If you are using the distributed solution and multitenancy mode, prior to using the **Endpoint Agents** section, you must select the tenant whose data you want to view.

*To select a tenant to manage in the **Endpoint Agents** section:*

1. In the upper part of the program web interface menu, click the arrow next to the name of the tenant.
2. In the drop-down list, select a tenant.

   Data for the selected tenant is displayed. If you want to select a different tenant, repeat the steps to select the tenant.

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 the distributed solution and multitenancy mode, the host table of Kaspersky Endpoint Agent can display the following information:

- 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:

- **Add to filter**.
- **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:

- **Add to filter**.
- **Exclude from filter**.
- **Copy value to clipboard**.

Viewing information about a host

To view information about a Kaspersky Endpoint Agent host:

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.
  - **Server name**—Name of the Central Node server.

- In the **Endpoint Agent** section:
  - **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**—Status of the Kaspersky Endpoint Agent program license key.

Filtering and searching hosts with Kaspersky Endpoint Agent by host name

To filter or search for Kaspersky Endpoint Agent hosts 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 Kaspersky Endpoint Agent hosts 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 the 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 Kaspersky Endpoint Agent hosts 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 Kaspersky Endpoint Agent hosts by IP address:

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 Kaspersky Endpoint Agent hosts by operating system version:

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 settings 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 Kaspersky Endpoint Agent hosts by Kaspersky Endpoint Agent version:

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 settings 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 Kaspersky Endpoint Agent hosts 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:

      - **Add to filter**, 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 the Kaspersky Endpoint Agent host filter for one or more filtering criteria:

1. Select the **Endpoint Agents** section in the window of the program web interface.
2. Click to 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. Users with the **Security auditor** role can view the settings of activity indicators of Kaspersky Endpoint Agent. Users with the **Senior security officer** or **Security officer** role 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.

To configure activity indicators for Kaspersky Endpoint Agent program:

1. Sign in to the program web interface under the **Local administrator**, **Administrator** or **Senior security officer** account.
2. In the window of the program web interface, select the **Settings** section, **Endpoint Agents** subsection.

3. In the fields under the section name, enter the number of days of inactivity of hosts with Kaspersky Endpoint Agent that you want to display as **Warning** and **Critical inactivity**.
4. Click **Apply**.

Activity indicators of Kaspersky Endpoint Agent will be configured.

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 doc dot docm docx dotx dotm docb
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

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 program web interface under an administrator account. If you have several Central Node components installed on the server, you need to create a request for each server with the Central Node component that you want to connect to the Sandbox component. If the Central Node component is deployed as a cluster, you can create a request for connection from any server in the cluster.

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.
- **Status**—Status of the connection to the Sandbox component.

Creating a request to connect to the server with the Sandbox component

To create a request to connect to the server with the Sandbox component through the program web interface:

1. Select the **Sandbox servers** section in the window of the program web interface.
2. In the upper-right corner of the window, click the **Add** button.

   This opens the **Sandbox server 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 **Add**.

The connection request is displayed in the web interface of the Sandbox component.

Enabling and disabling a connection with the Sandbox component

To make a connection with the Sandbox component active 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 row containing the relevant server in the **Status** column, perform one of the following actions:

   - If you want to activate a connection with the Sandbox component, set the toggle switch to **Enabled**.
   - If you want to disable a connection with the Sandbox component, set the toggle switch to **Disabled**.

3. Click **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 or the Kaspersky Security for Linux Mail Server Help.

   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 application 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 systems allowed to integrate:

1. Select the **External systems** section in the window of the program web interface.

   The **Server 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 **Maximum scan 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 **Maximum scan 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 application statistics is limited to the functionality provided by that license. If both license keys are added in the application, complete statistics is sent.

Before configuring the integration of Kaspersky Anti Targeted Attack Platform with the MDR application, you must download an archive with the configuration file from the MDR portal.

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 integration with MDR:

1. Log in to the program web interface with the administrator account.
2. Select the **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 integration with MDR:

1. Log in to the program web interface with the administrator account.
2. Select the **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 **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 information about user actions in the program web interface as well as alerts to a *SIEM system* already in use at your organization using the Syslog protocol.

You can use TLS encryption for data transmission.

If you have deployed the Central Node and Sensor components as a cluster, you can configure fault-tolerant integration with an external system using one of the following options:

- Using the Round Robin function.
- Configure the settings of the external system so that the external system switches between the IP addresses of the cluster servers if a network error occurs.

To configure the fault-tolerant integration with the external system:

1. Configure Round Robin on the DNS server for the domain name corresponding to the Central Node cluster.
2. Specify this domain name in the mail server settings.

   Integration with the mail server will be configured based on the domain name. The mail server will communicate with a random server in the cluster. If this server fails, the mail server will communicate with another healthy server in the cluster.

Enabling and disabling information logging to a remote log

You can configure the logging of information about user actions in the web interface and alerts to a remote log. The log file is stored on the server on which the SIEM system is installed. To write to the remote log, you must configure the integration with the SIEM system.

To enable or disable the logging of information about user actions in the web interface and alerts to the remote log:

1. In the window of the program web interface, select the **Settings** section, **SIEM system** subsection.
2. If you want to enable / disable the recording of information about user actions in the web interface to the remote log, do one of the following:
   - If you want to enable recording of information about user actions in the web interface, select the **Activity log** check box.
   - If you want to disable the recording of information about user actions in the web interface, clear the **Activity log** check box.
3. If you want to enable / disable the recording of information about alerts to the remote log, do one of the following:
   - If you want to enable recording of alert information, select the **Alerts** check box.
   - If you want to disable recording of alert information, clear the **Alerts** check box.

   You can select both check boxes simultaneously.
4. Click **Apply** in the lower part of the window.

   Information logging in the remote log is enabled or disabled.

Users with the **Security auditor** role can only view information about remote logging settings.

Configuring the main settings for SIEM system integration

To configure the main settings for SIEM system integration:

1. In the window of the program web interface, select the **Settings** section, **SIEM system** subsection.
2. Select the **Activity log** and/or **Alerts** check boxes.
   You can select one check box or both check boxes.
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 **Host ID** field, enter the host ID. The host with that ID is specified as the alert source in the log of the SIEM system.
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.

Users with the **Security auditor** role can only view information about the SIEM system integration settings.

Uploading a TLS certificate

To upload a TLS certificate for encrypting the connection with the SIEM system:

1. In the window of the program web interface, select the **Settings** section, **SIEM system** subsection.
2. In the **TLS encryption** section, click the **Upload** button.
   This opens the file selection window.
3. 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.
4. Click **Apply** in the lower part of the window.

The uploaded TLS certificate will be used to encrypt the connection with the SIEM system.

Enabling and disabling TLS encryption of the connection with the SIEM system

To enable or disable TLS encryption of the connection with the SIEM system:

1. In the window of the program web interface, select the **Settings** section, **SIEM system** subsection.
2. Select the **Activity log** and/or **Alerts** check boxes.

   You can select one check box or both check boxes.
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** setting can be used 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.

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.

  The current value of the field is `5.0.0-5201`.

- 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 |5.0.0-5201|url_web| URL from web
  detected|Low|
  ```

The body of a syslog message about an alert matches the information about that alert that is displayed in the program web interface. All fields are presented in the format `"<key>=<value>"`. Depending on whether the alert occurred in network traffic or mail traffic, and depending on the technology that generated the alert, various keys may be transmitted in the body of a syslog message. If the value is empty, the key is not transmitted.

The keys, as well as their values contained in a message, are presented in the table below.

Alert type	Alert name and description	Key and description of its value
file_web	File from web detected A file was detected in network traffic.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • rt = <date and time of alert>. • dst = <destination IP address>. • dpt = <destination port>. • src = <source IP address>. • spt = <source port>. • shost = <name of the host on which the file was detected>. • suser = <user name>. • fName = <name of the file within the compound object>. • fsize = <size of the file within the compound object (in bytes)>. • fileType = <format of the file within the compound object>. • fileHash = <MD5 hash of the file within the compound object>. • KasperskyLabKATAcompositeFilePath = <name of the compound object>. • KasperskyLabKATAcompositeFileSize = <total size of the compound object (in bytes)>. • KasperskyLabKATAcompositeFileHash = <MD5 hash of the compound object>. • KasperskyLabKATAfileSHA256 = <SHA256 hash of the compound object>. • cs2 = <technology that was used to detect the file>. • cs3Label = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • cs1 = <list of types of the detected objects according to the Kaspersky Lab classification>. • cs3 = <version of databases used to scan the file>. • app = <name of the application-level protocol> (HTTP(S) or FTP). • requestMethod = <HTTP request method> (only for the HTTP(S) protocol). • requestClientApplication = <User Agent of the client computer> (only for the HTTP(S) protocol). • request = <URL of the detected object> (only for the HTTP(S) protocol). • requestContext = <HTTP Referer header> (only for the HTTP(S) protocol).
file_mail	File from mail detected A file was detected in mail traffic.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • rt = <date and time of alert>. • fName = <name of the file within the compound object>. • fsize = <size of the file within the compound object (in bytes)>. • fileType = <format of the file within the compound object>. • fileHash = <MD5 hash of the file within the compound object>. • KasperskyLabKATAcompositeFilePath = <name of the compound object>. • KasperskyLabKATAcompositeFileSize = <total size of the compound object (in bytes)>. • KasperskyLabKATAcompositeFileHash = <MD5 hash of the compound object>. • KasperskyLabKATAfileSHA256 = <SHA256 hash of the compound object>. • KasperskyLabKATAmailEnvelopeFrom = <sender email address> (from the Received header). • KasperskyLabKATAmailFor = <recipient email address> (from the Received header). • KasperskyLabKATAmailRecievedFromIp = <IP address of the first server in the message delivery chain> (from the Received header). • cs2 = <technology that was used to detect the file>. • cs3Label = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • cs1 = <list of types of the detected objects according to the Kaspersky Lab classification>. • cs3 = <version of databases used to scan the file>. • externalId = <Email message ID>. • suser = <email address of sender>. • duser = <email addresses of recipients>. • msg = <message subject>.
ids	IDS event detected An alert was generated by the Intrusion Detection System module.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • requestMethod = <HTTP request method> (only for the HTTP(S) protocol). • requestClientApplication = <User Agent of the client computer> (only for the HTTP(S) protocol). • rt = <date and time of alert>. • dst = <destination IP address>. • dpt = <destination port>.

Alert type	Alert name and description	Key and description of its value
		• src = <source IP address>. • spt = <source port>. • proto = <name of the network-level protocol> (TCP or UDP). • cs1 = <type of the detected object according to the Kaspersky Lab classification>. • cs2Label = <name of the IDS rule>. • cs2 = <number of the IDS rule>. • cs3 = <Intrusion Detection System module database version>. • requestMethod = <HTTP request method> (only for the HTTP protocol). • requestClientApplication = <User Agent of the client computer> (only for the HTTP protocol). • request = <URL of the detected object>.
url_web	URL from web detected An alert was generated by URL Reputation technology or Sandbox in network traffic.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • rt = <date and time of alert>. • dst = <destination IP address>. • dpt = <destination port>. • src = <source IP address>. • spt = <source port>. • shost = <name of the host on which the file was detected>. • suser = <user name>. • cs1 = <list of categories to which the URL of the detected object belongs>. • requestMethod = <HTTP request method>. • requestClientApplication = <User Agent of the client computer>. • request = <URL of the detected object>. • requestContext = <HTTP Referer header>. • reason = <HTTP response code>.
url_mail	URL from mail detected An alert was generated by URL Reputation technology or Sandbox in mail traffic.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • rt = <date and time of alert>. • externalId = <Email message ID>. • suser = <email address of sender>. • duser = <email addresses of recipients>. • KasperskyLabKATAmailEnvelopeFrom = <sender email address> (from the Received header). • KasperskyLabKATAmailFor = <recipient address> (from the Received header). • KasperskyLabKATAmailRecievedFromIp = <IP address of the first server in the message delivery chain> (from the Received header). • msg = <message subject>. • request = <URL of the detected object>. • cs2 = <technology that was used to generate the alert> (Sandbox or URL Reputation). • cs3Label = <name of the virtual machine on which the file was detected> (only for Sandbox). • 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). • cs3 = <version of databases used to scan the file> (only for Sandbox).
dns	DNS request detected An alert was generated by URL Reputation technology in DNS traffic.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • rt = <date and time of alert>. • dst = <destination IP address>. • dpt = <destination port>. • src = <source IP address>. • spt = <source port>. • shost = <name of the host on which the file was detected>. • suser = <user name>. • cs2 = <list of URL categories to which the domain names belong>. • requestMethod = <type of DNS message> (request or response). • flexString1 = <type of record from the DNS request>. • dhost = <host name from the DNS request>. • cs1 = <list of domain names from the DNS response>.
file_endpoint	File from endpoint detected The alert was generated by the Kaspersky Endpoint Agent component on the user's computer and contains a file.	• dvchost = <name of server with the Central Node component>. • eventId = <alert ID>. • rt = <date and time of alert>. • src = <source IP address>. • shost = <name of the host on which the file was detected>. • fName = <name of the file within the compound object>. • fsize = <size of the file within the compound object (in bytes)>.

Alert type	Alert name and description	Key and description of its value
		• `fileType` = <format of the file within the compound object>. • `fileHash` = <MD5 hash of the file within the compound object>. • `KasperskyLabKATAcompositeFilePath` = <name of the compound object>. • `KasperskyLabKATAcompositeFileSize` = <total size of the compound object (in bytes)>. • `KasperskyLabKATAcompositeFileHash` = <MD5 hash of the compound object>. • `KasperskyLabKATAfileSHA256` = <SHA256 hash of the compound object>. • `cs2` = <technology that was used to detect the file>. • `cs3Label` = <name of the virtual machine on which the file was detected> (only for the Sandbox component). • `cs1` = <list of types of the detected objects according to the Kaspersky Lab classification>. • `cs3` = <version of databases used to scan the file>. • `app` = <name of the application-level protocol> (HTTP(S) or FTP). • `FilePath` = <path to the file on the computer with the Endpoint Sensors component>.
`iocScanning`	`IOC has tripped on endpoint` The alert was generated while carrying out an IOC scan of Kaspersky Endpoint Agent for Windows hosts. This type of alert is available if you are using KEDR functionality.	• `dvchost` = <name of server with the Central Node component>. • `eventId` = <alert ID>. • `rt` = <date and time of alert>. • `src` = <source IP address>. • `shost` = <name of the host on which the file was detected>. • `cs1` = <name of the IOC file by which the alert was generated>.
`taaScanning`	`TAA has tripped on events database` Alert resulting from the IOA analysis of events. This type of alert is available if you are using KEDR functionality.	• `dvchost` = <name of server with the Central Node component>. • `eventId` = <alert ID>. • `rt` = <date and time of alert>. • `shost` = <name of the host on which the alert was generated>. • `cs1` = <name of the IOA rule by which the alert was generated>.
`yaraScanningEP`	`YARA has tripped on endpoint` The alert was generated while carrying out a YARA scan of Kaspersky Endpoint Agent for Windows hosts. This type of alert is available if you are using KEDR functionality.	• `dvchost` = <name of server with the Central Node component>. • `eventId` = <alert ID>. • `rt` = <date and time of alert>. • `src` = <source IP address>. • `shost` = <name of the host on which the alert was generated>. • `cs1` = <name of the YARA rule by which the alert was generated>.
`heartbeat`	Periodic message containing the state of components.	• `dvchost` = <name of server with the Central Node component>. • `rt` = <event date and time>. • `KasperskyLabKATAcomponentName` = <name of the component>. • `KasperskyLabKATAcomponentState` = <status of the component> (`0` – OK, `>0` – Error).

Managing the application user activity log

Some user actions in the application web interface can cause errors in the operation of Kaspersky Anti Targeted Attack Platform. You can enable logging of user action information in the application web interface and if necessary, view the information by downloading log files.

Information about user actions in the web interface of the Sandbox component and the administrator menu of the Sensor component is recorded in the Sandbox and Sensor logs.

Enabling and disabling the recording of information in the activity log

To enable or disable the logging of information about user actions in the Kaspersky Anti Targeted Attack Platform web interface to the activity log:

1. Select the **Reports** section, **Activity log** subsection in the window of the program web interface.
2. Do one of the following:
   - Set the **Activity log** toggle switch to the **Enabled** position if you want to enable the logging of information about user actions in the program web interface.
   - Set the **Activity log** toggle switch to the **Disabled** position if you want to disable the logging of information about user actions in the program web interface.

     This function is enabled by default.

Information is logged for 30 days in the user_actions.log file. After 30 days, the user_actions.log file is saved on the Central Node server in the /var/log/kaspersky/apt-base/ directory with the name user_actions.log<month>. A new file named user_actions.log is created to record information for the current month. Each file is retained for 90 days and then deleted.

To view activity log files, you must download them.

You can configure the logging of information about user actions in the program web interface 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.

In distributed solution mode, information about user actions in the application web interface is recorded in the log of the same server for which the users are managing the web interface. Information about the actions of PCN server users that affect the settings of SCN servers is recorded in the PCN server log.

Users with the **Security auditor** role can only view the settings for logging information to the activity log.

Downloading the activity log file

To download the activity log file:

1. Select the **Reports** section, **Activity log** subsection in the window of the program web interface.
2. Click **Download**.

Log files are saved on your local computer in your browser's downloads folder. The files are downloaded as a ZIP archive.

In distributed solution mode, you can download log files only for the server for which you are managing the web interface.

Content and properties of CEF messages about user activity in the web interface

The header of each message 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.

  The current value of the field is `5.0.0-5201`.

- Event type.

  See the table below.

- Event name.

  See the table below.

- Event importance.

  Current field value: `Low`.

  Example:

  ```
  CEF:0|AO Kaspersky Lab|Kaspersky Anti Targeted Attack Platform|5.0.0-5201|tasks|Managing tasks|Low|
  ```

All fields of the CEF message have the `"<key>=<value>"` format. The keys, as well as their values contained in a message, are presented in the table below.

Event type	Event name and description	Key and description of its value
sensors	Managing the Sensor component Connecting the Sensor component to the Central Node server, modifying component settings.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>.
sb	Configuring integration with the Sandbox component Connecting the Sandbox component to the Central Node server.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>.
ex_integration	Configuring integration with external systems Configuring integration with external systems.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>.
ksn_kpsn_mdr	Participation in KSN, KPSN and MDR Configuring participation in Kaspersky Security Network, enabling or disabling the usage of Kaspersky Private Security Network, and configuring integration with Kaspersky Managed Detection and Response.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>.
yara	Managing YARA rules Operations with YARA rules.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>. • device external ID = <ID of the host in distributed solution mode>. • cs1label = <name of the uploaded file>.
ioc	Managing indicator of compromise Operations with IOC rules.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>. • deviceExternalID = <identifier of the host in distributed solution mode>.
ids	Managing IDS rules Operations with IDS rules.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>. • deviceExternalID = <identifier of the host in distributed solution mode>.
taa	Managing TAA rules Operations with TAA (IOA) rules.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>.
prevention	Managing prevention rules Operations with prevention rules.	• dvs = <IP address of the server>. • eventId = <ID of the event>. • rt = <event date and time>. • src = <IP address of the user>. • user = <user name>. • cs1 = <event type>.

Event type	Event name and description	Key and description of its value
`exclusions`	`Managing scan exclusions` Operations with scan exclusion rules.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`tasks`	`Managing tasks` Operations with tasks.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`network_isolation`	`Network isolation of Endpoint Agent hosts` Network isolation of Endpoint Agent hosts.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`settings`	`Settings` Modifying Central Node server settings.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`settings`	`Settings` The set of virtual machine operating systems is changed to <version of the operating system set>.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>. • `cs1label` = <name of the server where the settings were updated>.
`mt`	`Managing CN, PCN and SCN servers` Modifying the settings of Primary Central Node and Secondary Central Node servers in distributed solution and multitenancy mode.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`user_account`	`Managing user accounts` Actions on user accounts.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`notifications`	`Sending notifications` Configuring email notifications.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.
`license`	`License` Managing the license key.	• `dvs` = <IP address of the server>. • `eventId` = <ID of the event>. • `rt` = <event date and time>. • `src` = <IP address of the user>. • `user` = <user name>. • `cs1` = <event type>.

If an operation is performed on over 30 objects simultaneously, only one entry is logged for this operation. The entry includes the information about the operation and the number of objects on which it was performed.

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.

The update functionality (including anti-virus signature updates and code base updates), as well as the KSN functionality may be unavailable in the territory of the USA.

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 a database update source:

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.
2. In the **Database update** section, in the **Update source** drop-down list, select one of the following values:

   - **Kaspersky update server**.

     The program connects to Kaspersky update server over HTTP and downloads up-to-date databases.

   - **Kaspersky update server (secure connection)**.

     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 program database update package.

4. Click **Apply**.

The program database update source will be applied.

Updating databases manually

To start the database update manually:

1. In the window of the program web interface, select the **Settings** section, **General settings** subsection.

2. In the **Database update** section, click the **Start** button.

3. Click **Apply**.

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 archive passwords:

1. In the window of the program web interface, select the **Settings** section, **Passwords for archives** subsection.

2. In the **Passwords for 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.

Users with the **Security auditor** role can view the list of passwords for archives, but cannot edit it.

For security officers: Getting started with the application 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 application allows multiple security officers to work together.

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 / Security auditor**.

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 users with the **Senior security officer**, **Security officer**, and **Security auditor** roles provides the following sections:

- **Dashboard**. Contains Kaspersky Anti Targeted Attack Platform Monitoring data.
- **Alerts** Contains information about alerts in the network of the tenant to which you have access.
- **Threat Hunting**. Contains information about events found on hosts of the tenant to which you have access.
- **Tasks**. Contains information about tasks that you can use to manage files and programs on hosts.
- **Prevention**. Contains information about policies that you can use to manage preventions of files running on selected hosts.
- **Custom 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 computers with Kaspersky Endpoint Agent and their settings.

- **Reports**: **Generated Reports** and **Templates**. Contains a report builder and a list of generated reports about alerts.

- **Settings**: **IOC scanning schedule**, **Endpoint Agents**, **KPSN reputation database**, **Notification rules**, **VIP status**, **Exclusions**, **Passwords for 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 list of allowed objects, 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 a tenant to manage in the web interface of the program

If you are using distributed solution and multitenancy mode with a **Senior security officer** or **Security officer** account, before you begin using the web interface, you must select the tenant that you want to manage in the program web interface.

To select a tenant 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 name of the tenant.
2. In the **Select tenant** drop-down list, select a tenant.

   You can also start typing the name of the tenant in the search box and select the tenant from the list of search results.

All actions in the program web interface are applied to the selected tenant. If you want to select a different tenant, repeat the steps to select the tenant.

> Users with the **Security auditor** role cannot select a tenant to manage in the web interface.

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.

A *layout* is the appearance of the workspace of the program web interface window in the **Dashboard** section. You can add, delete, and move widgets in the layout, as well as configure the scale of widgets.

If you are using the distributed solution and multitenancy mode, this section displays information for the selected tenant.

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 lists attack vectors, alert importance levels, alert status, and technologies that generated the alerts. The right part of each widget displays the number of times the alerts were triggered during the selected period.

  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.

- **Sent to Sandbox by TAA rules**. 10 TAA (IOA) rules that most frequently cause Kaspersky Anti Targeted Attack Platform to send files for scanning by the Sandbox component.

The left part of each widget lists the domains, email addresses of recipients, IP addresses and email addresses of message senders, host names, and TAA (IOA) rule names. The right part of each widget displays the number of times the alerts were triggered during the selected period.

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. This opens the **Manage widgets** window; in that window, turn on the toggle switch next to the widget that you want to add.

The widget is 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 the upper part of the widget to drag and drop the widget to a different place in the layout.
6. Click **Save**.

The current layout is 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 is removed from the workspace of the program web interface window.
5. Click **Save**.

The widget is 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 is saved to the hard drive of your computer in the downloads folder of the browser.
6. Click **Close**.

Configuring the data display period in widgets

You can configure the display of data in widgets for the following periods:

- **Day**
- **Week**
- **Month**

To configure the display of data in widgets for a day (from 00:00 a.m. to 11:59 p.m.):

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 display data in 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 display data in the widget.

All widgets on the **Dashboard** page display data for the period you selected.

To display data display in widgets for a month (calendar month):

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 display data in 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" type widgets. The ☰ icon in the upper right corner of a widget means you can configure the scale for that widget.

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 ☰ 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 modified.

6. Repeat the steps for all widgets for which you want to set the display scale.

7. Click **Save**.

   The display scale of widgets is configured.

Basics of managing "Alerts" type widgets

You can configure the display scale for all "Alerts" type widgets.

The left part of each widget displays the legend for colors used in widgets.

Example:
The **Alerts by importance** widget displays the number of alerts of various importance.
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.
In the **Alerts by importance** widget, the following colors correspond to importance levels:

- 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 legend, the number of alerts of each type for the selected period is displayed.

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.
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. 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 tenant 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.

Users with the **Local administrator**, **Administrator**, or **Security auditor** roles can gain access to 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**, **Security officer**, or **Security auditor** roles can gain access to 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 gain access to information about the working condition of that SCN server for tenants to whose data the user has access.
- If you are using the distributed solution and multitenancy mode, and the user is managing the PCN server, the user can gain access to information about the working condition of the PCN server and all SCN servers connected to that server, for tenants to whose data the user has access.

For details about the working condition of program modules and components,

click **View details** to open the **System health** window.

In the **System health** window, one of the following icons is displayed depending on the working condition of the program modules and components:

- OK if the modules and components of the program are working normally.
- An icon with the number of problems (for example, 1) if problems are found that the administrator is recommended to pay attention to. 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:

- **Component health** contains information on the operational status of program modules and components, Quarantine, and database 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**—Status 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.
- **Connection with servers**—Status 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.

Viewing the alert table

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.

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 100,000 alerts for each component.
- All other alerts have a maximum of 20,000 alerts for each module or component.

If you are using the 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**, **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 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. **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 tenant that 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** for new alerts
    - **In process** for alerts that are already being processed by Kaspersky Anti Targeted Attack Platform user
    - **Rescan** for 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:
  - **Add to filter**.
  - **Exclude from filter**.
  - **Copy value to clipboard**.
- MD5 hash:
  - **Add to filter**.
  - **Exclude from filter**.
  - Find events.
  - **Find on TIP**.
  - **Create prevention rule**.
  - **Copy value to clipboard**.

- SHA256 hash:
  - **Add to filter**.
  - **Exclude from filter**.
  - Find events.
  - **Find on TIP**.
  - **Create prevention rule**.
  - **Copy value to clipboard**.
- Destination IP address: **Find events**.
- Alert state:
  - **Assign to me**.
  - **Close alert**.

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.

Configuring the alert table display

You can show or hide columns and change the order of columns in the alert table.

To configure the alert table display:

1. Select the **Alerts** section in the window of the application web interface.

   This opens the table of alerts.

2. In the heading part of the table, click  .

   This opens the **Customize table** window.

3. If you want to show a column in the table, select the check box next to the name of the parameter that you want displayed in the table.

   If you want to hide a parameter in the table, clear the check box.

   > At least one check box must be selected.

4. If you want to change the order of columns in the table, move the mouse cursor to the row with the relevant parameter, click  and move the row to its new place.
5. If you want to restore default table display settings, click **Restore defaults**.
6. Click **Apply**.

The alert table display is configured.

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 the distributed solution and multitenancy mode, you cannot 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**, **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 by 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.

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 by importance:

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 by category of the detected object:

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 by 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**
   - **Autosend to Sandbox**
   - **TAA (IOA) rule**
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 **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 **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 tenant 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 by 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 are not being processed by any user yet.
   - **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**, **Source**, and **State** columns.

To sort 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 **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 in order of processing **New** - **Rescan** - **In process** - **Closed**.
   - ↓ to sort alerts in order of processing **Closed** - **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:

   - **Add to filter**, 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 the alert filter for one or more filtering criteria:

1. Select the **Alerts** section in the window of the program web interface.

   This opens the table of alerts.

2. Click 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 the processes using the Kaspersky Endpoint Agent program installed on computers belonging to the corporate IT infrastructure.

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 (32-bit), Windows 7 (64-bit), Windows 10 (64-bit), and CentOS 7.8 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 alert details:

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 tenant that 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 object:

- 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 TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

  Click **Create prevention rule** to prevent the file from running.

  Click **Download** 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 TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Create 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 TIP**.
- **Find on virustotal.com**.
- **Find events**.
- **Find alerts**.
- **Create prevention rule**.
- **Copy value to clipboard**.

- **Sender email**—Email address from which the message containing the file was sent.
- **Recipient email**—One or more email addresses to which the message containing the file was sent.
- **Original sender email**—Source email address from which the message containing the file was sent.
  This field is populated with data from the 'Received' header.
- **Original recipient email**—Source email address(es) to which the message containing the file was sent.
  This field is populated with data from the 'Received' header.
- **Subject**—Message subject.
- **Sender server IP** —IP address of the first mail server in the message delivery chain.
  Clicking the **Sender server IP** link with opens a list in which you can select one of the following actions:
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.
- **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 application 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 Kaspersky TIP by URL**.
  - **Find on Kaspersky TIP by domain name**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

- **Referer**—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 application.

  Clicking the link with **Destination IP** opens a list in which you can select one of the following actions:

  - **Find on Kaspersky 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**—Results of streaming scans of files and objects received at the Central Node, or results of scanning Kaspersky Endpoint Agent hosts. Possible values:

    - Category of the detected file in YARA rules (for example, category name susp_fake_Microsoft_signer can be displayed).

      Displayed for streaming scans.

      Click **Create prevention rule** to prevent the file from running.

The **Find on TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

- Path to the file and/or name of the memory dump.

  Displayed when scanning Kaspersky Endpoint Agent hosts.

  Clicking the link with the file path opens a list in which you can select one of the following actions:

  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

You can click **Create task** to create the following tasks:

- **Get data** → **File**, **Disk image**, **Memory dump**
- **Delete file**
- **Quarantine file**

Click **Create prevention rule** to prevent the file from running.

The **Find on TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

You can click **View in quarantine** to display quarantined object details.

- **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 TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

  Click **Create 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 TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

Click **Create prevention rule** to prevent the file from running.

Click **Download** 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 **All alert-related 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 followed on the user's 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.

  If the alert is created for a file extracted from traffic, the URL specifies the protocol used to transmit the traffic from which the file was extracted. Possible protocols: HTTP, HTTPS, FTP, SMTP, POP3, SMB, NFS.

Clicking the link with the URL opens a list in which you can select one of the following actions:

- **Find on Kaspersky TIP by URL**.
- **Find on Kaspersky 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 TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Create 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 TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

  Clicking a link in the **URL** column opens a list in which you can select one of the following actions:
  - **Find on TIP by URL**.
  - **Find on 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 TIP**.
  - **Find events**.
  - **Find alerts**.
  - **Copy value to clipboard**.

Clicking a link in the **URL** column opens a list in which you can select one of the following actions:

- **Find on TIP by URL**.
- **Find on 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 a link in the **DNS name** or **Host** columns opens a list in which you can select one of the following actions:

  - **Find on 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

Depending on the type of processed object, the indicator of compromise search result window can display the following information:

- **ARP protocol**:
  - IP address from the ARP table.
  - Physical address from the ARP table.
- **DNS record**:
  - Type and name of the DNS record.
  - IP address of the protected computer.

- **Windows Log event**:
  - Entry ID in the event log.
  - Data source name in the log.
  - Log name.
  - User account.
  - Event time.
- **File**:
  - MD5 hash of the file.
  - SHA256 hash of the file.
  - Full name of the file (including path).
  - File size.
- **Port**:
  - Remote IP address with which a connection was established at the time of the scan.
  - Remote port with which a connection was established at the time of the scan.
  - IP address of the local adapter.
  - Port open on the local adapter.
  - Protocol as a number (in accordance with the IANA standard).
- **Process**:
  - Process name.
  - Process arguments.
  - Path to process file.
  - Windows ID (PID) of the process.
  - Windows ID (PID) of the parent process.
  - Name of the user account that started the process.
  - Date and time when the process started.
- **Service**:
  - Service name.
  - Service description.

- Path and name of the DLL service (for svchost).
- Path and name of the executable file of the service.
- Windows ID (PID) of the service.
- Service type (for example, kernel driver or adapter).
- Service status.
- Service run mode.

- **User**:
  - User account name.
- **Volume**:
  - Volume name.
  - Volume letter.
  - Volume type.
- **Registry**:
  - Windows registry value.
  - Registry hive value.
  - Path to registry key (without hive or value name).
  - Registry parameter.
- **Environment variables**:
  - Physical (MAC) address of the protected computer.
  - System (environment).
  - OS name with version.
  - Network name of the protected device.
  - Domain and group to which the protected computer belongs.

The **IOC** section displays the structure of the IOC file. If the processed object matches a condition of the IOC rule, that condition is highlighted. If the processed object matches multiple conditions, the text of the whole branch is highlighted.

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.
- **IP**—IP address of the computer where the event occurred.

  If you are using dynamic IP addresses, the field displays the IP address assigned to the computer at the moment when the alert was created or updated.

  The program does not support IPv6. If you are using IPv6, the IP address of the computer is not displayed.
- **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 detection information:

- Date and time of alert modification.
- Author of modifications.

  For example, **System** or the application 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 details 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 produced by AM (Anti-Malware Engine), SB (Sandbox), YARA, IOC, IDS (Intrusion Detection System), NDR: IDS, and AA (Aggregated Alerts) technologies that is displayed in the right part of the window includes recommendations on processing these alerts.

To view alert details:

1. Select the **Alerts** section in the window of the application 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 similar 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 **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 **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 similar events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the **Scan: 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 similar 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 TAA 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 similar 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 rule name (TAA alerts)**. Clicking the link opens the **Alerts** alert table in a new browser tab; the alerts are filtered by **Detected** and **Technologies** columns, that is, the name of the TAA (IOA) rule that was used to create the alert, and the name of the **(TAA) Targeted Attack Analyzer** technology.

- **By rule name (SB alerts)**. Clicking the link opens the **Alerts** alert table in a new browser tab; the alerts are filtered by **Detected** and **Technologies** columns, that is, the name of the TAA (IOA) rule that was used to create the alert, and the name of the **(SB) Sandbox** technology.

- Under **Investigation**, select **Find similar 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 similar 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 **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 **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 similar EPP events**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the **Scan: 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 similar 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 similar alerts by host name**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Source** column. The host name from the alert you are working on is highlighted in yellow.

- Under **Qualifying**, select **Find similar 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 after** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.
2. In the **Exclusions for 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.

   You can use a proxy server to let Kaspersky Endpoint Agent for Windows connect to Kaspersky Anti Targeted Attack Platform. When you add this proxy server to exclusions, network resources that can be accessed through the proxy server are also added to exclusions. If network resources that are accessed through the proxy server are added to exclusions, but the proxy server itself is not, such exclusions do not work.
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** and repeat the steps to fill in the **Traffic direction**, **IP** and **Ports** fields.
6. Click **Save**.

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 similar 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 **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 **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 similar alerts by host name**. Click the link to display the **Threat Hunting** event table in a new browser tab. In the search criteria, the **Scan: 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 similar 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.

- In the **Quick response** section, select **Isolate <host name>**. This opens the network isolation rule creation window.

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 similar alerts by IP address**. Click the link to display the **Alerts** alert table in a new browser tab. The alerts are filtered by the **Source** column. The host name or IP address from the alert you are working on is highlighted in yellow.

- Under **Qualifying**, select **Find similar 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 exclusions**.

  This opens the **Add IDS rule to exclusions** 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**.

  The IDS rule is added to exclusions and is displayed in the exclusion list in the **Settings** section, **Exclusions** subsection on the **IDS** tab in the application web interface.

- Under **Investigation**, select **Find similar 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 similar events by IP address**. 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 managing the program web interface using a **Senior security officer** or **Security officer** account, you can take the following actions on alerts:

- Assign an alert to yourself 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.

Users with the **Security auditor** role can view information about alerts but cannot edit this information.

Assigning alerts to a specific user

Users with the **Senior security officer** and **Security officer** roles can assign an alert or multiple alerts to themselves or to another user of the program web interface with the **Senior security officer** and **Security officer** roles.

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 next to the alert or 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 panel that appears in the lower part of the window, click the arrow to the right of the **Assign to** button to expand the user list.

4. Select the user to whom you want to assign the alerts.

   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 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.

Users with the **Security auditor** role cannot assign alerts to themselves or to other users of the program web interface. Users with the **Senior security officer** and **Security officer** roles also cannot assign alerts to users with the **Security auditor** role.

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 **Close alert**.

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.

   Expand the list of actions. In the upper right corner of the window, click the arrow to the right of the button showing the alert status.

   This opens the list of actions.

3. In the action list, select **Close alert**.

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.

If an alert based on TAA (IOA), IDS, or URL technology that is similar to a processed alert is received within the day (from 00:00 a.m. to 11:59 p.m.), the program will either create a new alert or update the information about an identical alert with the **New** or **In process** status.

Users with the **Security auditor** role cannot assign and process alerts.

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 **Close alert** 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.

If an alert based on TAA (IOA), IDS, or URL technology that is similar to a processed alert is received within the day (from 00:00 a.m. to 11:59 p.m.), the program will either create a new alert or update the information about an identical alert with the **New** or **In process** status.

Users with the **Security auditor** role cannot assign and process alerts.

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 toggle the VIP status for 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 for alerts for which you want to change the VIP status.

   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, in the pane that appears in the lower part of the window, in the **Mark as VIP** drop-down list, select **Mark as non-VIP**.

   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** and **Security auditor** roles can view all events with the VIP status by filtering alerts by VIP status.

Adding a comment to an alert

Users with the **Senior security officer** and **Security officer** roles can add 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 field under the **Change log** section, enter a comment for the alert.

4. Click **Add**.

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.

Users with the **Security auditor** role can view comments for alerts but cannot edit the comments.

Events database threat hunting

When managing the program web interface, you can generate search queries and use IOC files to search the events database for threats, for tenants to whose data you have 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.

Users with the **Senior security officer**, **Security officer** roles can also create TAA (IOA) rules based on event search conditions.

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 selected **Custom range**:

   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.

   If you are using the distributed solution and multitenancy mode, found events are grouped in tiers: Server – Tenant names – Server names.

6. Click the name of the server for which you want to view events.

The host table of the selected server is displayed. Event grouping levels are displayed above the table.

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 an event search criterion.

   Available event search criteria

   - Under **General details**:
     - Host is the host name.
     - HostIP is the IP address of the host.
     - EventType is the type of the event.
     - UserName is the name of the user.
     - OsFamily is the family of the operating system.
     - OsVersion is the version of the operating system being used on the host.
   - Under **TAA properties**:
     - IOAId is the TAA (IOA) rule ID.
     - IOATag is the 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.
     - IOATechnique is the MITRE technique.
     - IOATactics is the MITRE tactic.
     - IOAImportance is the importance level that is assigned to an event generated using this TAA (IOA) rule.
     - IOAConfidence is the level of confidence depending on the likelihood of false alarms caused by the rule.

- Under **File properties**:
  - CreationTime is the event creation time.
  - FileName is the name of the file.
  - FilePath is the path to the directory where the file is located.
  - FileFullName is the full path to the file. Includes the path to the directory and the file name.
  - ModificationTime is the file modification time.
  - FileSize is the size of the file.
  - MD5 is the MD5 hash of the file.
  - SHA256 is the SHA256 hash of the file.
  - SimilarDLLPath is the next DLL on the search path. A malicious DLL placed in a directory on the standard search path to make the operating system load it before the original DLL.
- Under **Linux processes**:
  - LogonRemoteHost is the IP address of the host that initiated remote access.
  - RealUserName is the name of the user assigned when the user was registered in the system.
  - EffectiveUserName is the user name that was used to log in to the system.
  - Environment is system environment variables.
  - ProcessType is the type of the process.
  - OperationResult is the type of the operation.
- Under **Process started**:
  - PID is the process ID.
  - ParentFileFullName is the path to the parent process file.
  - ParentMD5 is the MD5 hash of the parent process file.
  - ParentSHA256 is the SHA256 hash of the parent process file.
  - StartupParameters is the options that the process was started with.
  - ParentPID is the parent process ID.
- Under **Remote connection**:
  - HTTPMethod is the HTTP request method. For example, Get, Post, or Connect.
  - ConnectionDirection is the direction of the connection (inbound or outbound).

- LocalIP is the IP address of the local computer from which the remote connection attempt was made.
- LocalPort is the IP address of the local computer from which the remote connection attempt was made.
- RemoteHostName is the name of the computer that was the target of the remote connection attempt.
- RemoteIP is the IP address of the computer that was the target of the remote connection attempt.
- RemotePort is the port of the computer that was the target of the remote connection attempt.
- URI is the address of the resource to which the HTTP request was made.

- Under **Registry modified**:
  - RegistryKey is the registry key.
  - RegistryValueName is the name of the registry value.
  - RegistryValue is the data of the registry value.
  - RegistryOperationType is the type of the operation with the registry.
  - RegistryPreviousKey is the previous registry key.
  - RegistryPreviousValue is the previous name of the registry value.
- Under **System event log**:
  - WinLogEventID is the type ID of the security event in the Windows log.
  - LinuxEventType is the type of the event.
  - WinLogName is the name of the log.
  - WinLogEventRecordID is the log entry ID.
  - WinLogProviderName is the ID of the system that logged the event.
  - WinLogTargetDomainName is the domain name of the remote computer.
  - WinLogObjectName is the name of the object that initiated the event.
  - WinlogPackageName is the name of the package that initiated the event.
  - WinLogProcessName is the name of the process that initiated the event.
- Under **Detect and processing result**:
  - DetectName is the name of the detected object.
  - RecordID is the ID of the triggered rule.
  - ProcessingMode is the scanning mode.
  - ObjectName is the name of the object.

- ObjectType is the type of the object.
- ThreatStatus is the detection mode.
- UntreatedReason is the event processing status.
- ObjectContent (for AMSI events too) is the content of the script sent for scanning.
- ObjectContentType (for AMSI events too) is the type of script content.

- Under **Console interactive input**:
  - InteractiveInputText is the text entered on the command line.
  - InteractiveInputType is the input type (console or pipe).
- Under **File changed**:
  - FileOperationType is the type of the file operation.
  - FilePreviousPath is the path to the directory where the file was previously located.
  - FilePreviousFullName is the full name of the file including the path to the directory where the file was previously located and/or the previous file name.
  - DroppedFileType is the type of the modified file.

3. In the drop-down list, select a comparison operator.

   Available 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 selected **Custom range**:

   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.

    If you are using the distributed solution and multitenancy mode, found events are grouped in tiers: Server – Tenant names – Server names.

11. Click the name of the server for which you want to view events.

The host table of the selected server is displayed. Event grouping levels are displayed above the table.

Sorting events in the table

You can sort events in the table by the **Event time**, **Event type**, **Host**, and **User name** columns.

To sort events in the event table:

1. Select the **Threat Hunting** section in the program web interface window.

   This opens the **Threat Hunting** window.

2. Define the criteria for searching events in design mode or source code mode.

   The table of events that satisfy the search criteria is displayed.

3. If you want to sort events by time, click one of the icons to the right of the **Event time** column name:

   - ↑ to display newer events at the top of the table.
   - ↓ to display older events at the top of the table.

4. If you want to sort events by the event type name, click one of the icons to the right of the **Event type** column heading:

   - ↑ to sort alphabetically, A–Z.
   - ↓ to sort alphabetically, Z–A.

5. If you want to sort events based on the names of host on which the alerts were generated, click one of the icons to the right of the **Host** column name:

   - ↑ to sort alphabetically, A–Z.
   - ↓ to sort alphabetically, Z–A.

6. If you want to sort events based on the user names of hosts, click one of the icons on the right of the **User name** column name:

   - ↑ to sort alphabetically, A–Z.
   - ↓ to sort alphabetically, Z–A.

7. If you want to group events based on the names of hosts or by the event type name, click one of the values in the **Group by** drop-down list:

   - **Group by host name** if you want to group events by the names of hosts.
   - **Group by event type** if you want to group events by the names of event types.

   If events were sorted by the **Host** or **Event type** field, the sorting result is cleared when events are grouped by a similar attribute. To return to the sorting results, select the **Group by** value from the **Group by** drop-down list.

By default, events in the table are sorted by time, with the newest events at the top of the table.

You can sort events based on one attribute only.

When sorting by event type in a foreign language, events are sorted based on the internal name of the event type in English.

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 exclusions**.
- **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 is running in Report only mode**.
   - **Failed to back up object**.
   - **Failed to copy object**.
   - **Device not ready**.
   - **Object blocked**.
   - **No rights to perform action**.
   - **Object not curable**.
   - **Object not overwritable**.
   - **Object not found**.
   - **No free space on disk**.
   - **Processing canceled**.
   - **Processing postponed**.

- **Processing task stopped**.
- **Error reading data**.
- **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 that 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 TAA (IOA) rule based on event search conditions

To create a TAA (IOA) rule 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 **Save as TAA (IOA) rule**.

   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 **Custom 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 TAA (IOA) rule that you have created earlier will be unable to mark events by these fields.

Users with the **Security auditor** and **Security officer** roles cannot create TAA (IOA) rules based on event search conditions.

Event information

If you are using the distributed solution and multitenancy mode, when managing the program using the web interface, you can view event information for those tenants to whose data you 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.

To enable the display of events for all tenants:

1. Select the **Threat Hunting** section in the program web interface window.
2. Turn on the **Search in all tenants** toggle switch.

   The table of events displays events for all tenants.

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. You can sort events in the table by the **Event time**, **Event type**, **Host**, and **User name** columns.

If you are using the distributed solution and multitenancy mode, events in the table are grouped by hosts of the selected servers and tenants.

The table of events contains the following information:

1. **Event time**—Date and time when the event was detected.
2. **Event type**, for example, **Process started**.
3. **Host**—Name of the host on which the alert was generated.
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.

In the events table, the **Details** column displays the set of data for each type of event in the **Event type** column (see the table below).

Set of data in the **Details** column for each event type in the **Event** column

Event type	Details
Process started	Name of the process file that was started. SHA256- and MD5 hash.
Module loaded	Name of the dynamic library that was loaded. SHA256- and MD5 hash.
Connection to remote host	URL to which a remote connection attempt was made. Name of the file that attempted to establish a remote connection.
Blocked application (prevention rule)	Name of the file of the application that was blocked from starting. SHA256- and MD5 hash.
Document blocked	Name of the document that was blocked from starting. SHA256- and MD5 hash.
File changed	Name of the created file. SHA256- and MD5 hash.
System event log	Channel for recording events in the system log. Event type ID.
Registry modified	Name of key in registry. `<name of the variable in the key>=<value of the variable>`.
Port listened	Server address and port. Name of the file of the process that listens to the port.
Driver loaded	File name of the driver that has been loaded. SHA256- and MD5 hash.
Scan: detect	Alert
Scan: detect processing result	Alert processing result.
AMSI scan	AMSI scan results.
Process: interpreted file run	Interpreted run of a file.
Process: console interactive input	Interactive input of commands in the console.

Information about the **AMSI scan** event is available when Kaspersky Anti Targeted Attack Platform is integrated with Kaspersky Endpoint Agent for Windows 3.10 or later and when Kaspersky Endpoint Agent is integrated with Kaspersky Endpoint Security for Windows 11.5 or later. If Kaspersky Endpoint Security for Windows is not installed on the computer and is not integrated with the Kaspersky Endpoint Agent program, information about the **AMSI scan** event is not logged in the event database and is not displayed in the Kaspersky Anti Targeted Attack Platform web interface.

The Central Node server generates a **Scan: detect** and a **Scan: 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 Kaspersky Endpoint Agent program, information about these events is not logged in the event database and is not displayed in the Kaspersky Anti Targeted Attack Platform web interface.

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 value in the cell, you can perform one of the following actions:

- For all values in the cell:
  - **Add to filter**.
  - **Exclude from filter**.
  - **Copy value to clipboard**.
- Host name:
  - Find events.
  - Find alerts.
  - Isolate from network.
- File name:
  - Kill process.
  - Kill by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- MD5 hash:
  - Find events.
  - Find alerts.
  - Find on TIP.
  - Create prevention rule.
  - Find in Storage.
- SHA256 hash:
  - Find events.
  - Find alerts.

- Find on TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.

Configuring the event table display

You can show or hide columns and change the order of columns in the event table.

To configure the event table display:

1. Perform an event search in builder mode or source code mode.

   The event table is displayed.

2. In the heading part of the table, click  .

   This opens the **Customize table** window.

3. If you want to show a column in the table, select the check box next to the name of the parameter that you want displayed in the table.

   If you want to hide a parameter in the table, clear the check box.

   > At least one check box must be selected.

4. If you want to change the order of columns in the table, move the mouse cursor to the row with the relevant parameter, click  and move the row to its new place.

5. If you want to restore default table display settings, click **Default**.

6. Click **Apply**.

The display of the event table is configured.

Viewing information about an event

To view event details:

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 the distributed solution and multitenancy mode and want to enable the display of events for all tenants, turn on the **Search in all tenants** 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 view the 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 started:

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 for users with the **Senior security officer** role.

You can follow the following recommendations:

- **Isolate <host name>** – isolate the host with Kaspersky Endpoint Agent program where the event was detected from the network. Applies to all event types.
- **Create prevention rule** – prohibit the execution of the file that was detected in the event. Applies to all event types except **System event log** and **Host name changed**.
- **Create task** — create a task. Applies to all event types except **System event log** 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 by unique PID**.
  - **Delete file**.

    - Get file.
    - Get forensics.
    - Quarantine file.
- **Copy value to clipboard**.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- **Add to filter**.
- **Exclude from filter**.
- Find on 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:

- Find events.
- Find alerts.
- Find on TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create 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.
- Run the following tasks:
    - Kill process.
    - Delete file.
    - Get file.
    - Get forensics.

- Quarantine file.
- Run program.

- **Copy value to clipboard**.

Users with the **Security auditor** and **Security officer** roles are not shown recommendations for processing events.

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 after** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.

3. In the **Exclusions for 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.

   You can use a proxy server to let Kaspersky Endpoint Agent for Windows connect to Kaspersky Anti Targeted Attack Platform. When you add this proxy server to exclusions, network resources that can be accessed through the proxy server are also added to exclusions. If network resources that are accessed through the proxy server are added to exclusions, but the proxy server itself is not, such exclusions do not work.

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** 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.

Users with the **Security auditor** and **Security officer** roles cannot isolate a host from the network.

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 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 display a notification about prevention rule triggering to the user of the computer on which the prevention is applied, select the **Notify user about blocking file 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 **Add**.

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 blocking file execution** check box and an attempt is made to execute a file prevented from running, the user is notified that an execution prevention rule was triggered by this file.

Users with the **Security auditor** and **Security officer** roles cannot prevent file execution.

Following a recommendation to create a task

To follow a recommendation to create a task:

1. Click **Create task**, and in the recommendation box, expand the list of task types.
2. Select a task type:
   - Kill process
   - Get forensics
   - Start YARA scan
   - Service management
   - Get process memory dump
   - Get NTFS metafiles
   - Run program
   - Get file
   - Delete file
   - Quarantine file
   - Restore file from quarantine

   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**, **Delete file**, **Start YARA scan**, or **Service management** 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 **Add**.

The task is created.

Information about the created task is displayed in the **Tasks** section of the web interface.

Users with the **Security auditor** and **Security officer** roles cannot create tasks.

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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **File**—Process file name.
  - **Process ID**—Process identifier.
  - **Launch parameters**—Process startup settings.
  - **MD5**—MD5 hash of the process file.
  - **SHA256**—SHA256 hash of the process file.
  - **Size**—Size of the process file.
  - **Event time**—Process start time.
  - **Time created**—Process file creation time.
  - **Time modified**—Time of last modification of the process file.

  If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **Process started** section also displays the **Command** field for the command that was used to run the process.
- **Details** section:
  - **Program name**—For example, the 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 subject**—Organization that issued the digital certificate of the file.
- **Signature validation result**—For example, "Invalid" or "OK".
- **Attributes**—File attribute in accordance with the Windows classification. For example, A (archive), D (directory), or S (system file).

If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **Details** section also includes the following fields:

- **Attributes**—Attributes of the process file.
- **Process type**—For example, exec.
- **Environment variables**—Environment variables of the process.
- **Real user name**—Name of the user assigned when registering in the system.
- **Real group name**—Group to which the user belongs.
- **Effective user name**—User name that was used to log in to the system.
- **Effective group name**—Group of the user whose name was used to log in to the system.
- **Owner user name**—Name of the user that created the process file.
- **Owner group name**—Name of the group whose users can modify or delete the file of the process.
- **File permitted capabilities**—Permissions that can be used to gain access to the process file.
- **File inheritable capabilities**—Permissions that an user group has to perform operations on the parent directory of the process file.
- **File effective capabilities**—Permissions that are relevant to the process file at the current moment.

- **Event initiator** section:
  - **File**—Path to the parent process file.
  - **Process ID**—Identifier of the parent process.
  - **Launch parameters**—Parent process startup settings.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

    If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **Parent process** section also displays the **Command** field for the command that was used to run the parent process.
- **System info** section:
  - **Host name**—Name of the host on which the process was started.
  - **Host IP**—IP address of the host on which the process was started.

If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

- **Account type**—Type of the account that ran the process. For example, administrator.
- **Logon type**—For example, using a running service.
- **User name**—Name of the user that started the process.
- **OS name**—Version of the operating system that is being used on the host.

  If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **System info** section also displays the **Logon from remote host** field for the name of host from which the remote logon was performed.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Agent for Linux records in the event database, you can click the links with the file name or file path to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the Get file task.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Agent for Linux records in the event database, you can click the link with the host name to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the following tasks:
  - Get 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "Process terminated" event

The window displaying information about **Process terminated** events contains the following details:

- Tree of events.
- Actions that can be performed to handle an event.
- **Process terminated** 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **File**—Process file name.
  - **Process ID**—Process identifier.
  - **Launch parameters**—Process startup settings.

    If the event was logged in the event database by Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Mac, instead of the **Launch parameters** field, the **Command** field is displayed, that is, the command that was used to run the process.
  - **MD5**—MD5 hash of the process file.
  - **SHA256**—SHA256 hash of the process file.
  - **Size**—Size of the process file.
  - **Event time**— Process termination time.
- **Event initiator** section:
  - **File**—Path to the parent process file.
  - **Process ID**—Identifier of the parent process.

- **Launch parameters**—Parent process startup settings.

  If the event was logged in the event database by Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Mac, instead of the **Launch parameters** field, the **Command** field is displayed, that is, the command that was used to run the parent process.

- **MD5**—MD5 hash of the parent process file.

- **SHA256**—SHA256 hash of the parent process file.

- **System info** section:

  - **Host name**—Name of the host on which the process was started.

  - **Host IP**—IP address of the host on which the process was started.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The application does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

  - **User account type**—Type of the account that terminated the process. For example, administrator.

  - **User name**—Name of the user that started the process.

  - **OS version**—Version of the operating system that is being used on the host.

  If the event was logged in the event database by Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Mac, the **System info** section also displays the **Logon from remote host** field for the name of host from which the remote logon was performed.

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:
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Security for Linux or Kaspersky Endpoint Security for Mac recorded in the event database, you can click the links with the file name or file path to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the Get file task.
- **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**.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - **Kill process**.
  - **Delete file**.
  - **Quarantine file.**
  - **Run application**.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Security for Linux recorded in the event database, you can click the link with the host name to open 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.**
  - Run application.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Security for Mac recorded in the event database, you can click the links with the file name or file path to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the Get file task.
- **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 Kaspersky TIP
- **Find in Storage**.
- **Create 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 Kaspersky TIP
- **Find on virustotal.com**.
- Find in Storage.
- Create 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **File**—Name of the loaded module file.
  - **MD5**—MD5 hash of the loaded module file.
  - **SHA256**—SHA256 hash of the loaded module file.
  - **Size**—Size of the loaded module.
  - **Event time**—Time when the module was loaded.
- **Details** section:
  - **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, Example File.
  - **Signature subject**—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.
  - **Next DLL in bypass path**—The field contains the path to the DLL library that could have been loaded instead of the existing library.

    The field is displayed if the following conditions are satisfied:
    - The source of the loaded DLL is not trusted.
    - A folder in the standard search path contains a library with the same name but a different hash.

    Kaspersky Anti Targeted Attack Platform receives the data required to populate the **Next DLL in bypass path** field only when Kaspersky Anti Targeted Attack Platform is integrated with the Kaspersky Endpoint Agent for Windows program version 3.10. When integrating the program with older versions of the Kaspersky Endpoint Agent program, the field is not displayed in the event information.

- **Event initiator** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.
- **System info** section:
  - **Host name**—Name of the host on which the module was loaded.
  - **Host IP**—IP address of the host on which the module was loaded.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user that loaded the module.
  - **OS name**—Version of the operating system being used on the host.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **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.

- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "Remote connection" event

The window showing information about **Connection to remote host** events contains the following details:

- Tree of events.
- Recommendations for processing an event.

- **Connection to remote host** 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **Connection direction** is the direction of the connection (inbound or outbound).
  - **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.
  - **Event time**—Time of the remote connection attempt.
- **Event initiator** section:
  - **File**—Name of the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.
- **System info** section:
  - **Host name**—Host name from which a remote connection attempt was made.
  - **Host IP**—IP address of the host from which a remote connection attempt was made.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user that attempted to establish a remote connection.
  - **OS name**—Version of the operating system being used on the host.

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 by unique PID.

    - Delete file.
    - Get file.
    - Get forensics.
    - Quarantine file.
- **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.
- Run the following tasks:
    - **Get data** → File, Forensics, Disk image, Memory dump.
    - Kill process.
    - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.

- Create 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 **Blocked application (prevention rule)** type, displays the following details:

- Tree of events.
- Recommendations for processing an event.
- **Blocked application (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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **File**—Name of the file that was prevented from running.
  - **Launch parameters**—Parameters that were used for the attempt to run the file.
  - **MD5**—MD5 hash of the file that was prevented from running.
  - **SHA256**—SHA256 hash of the file that was prevented from running.
  - **Size**—Size of the file that was prevented from running.
  - **Event time**—Time when the file run prevention was triggered.
- **Details** section:
  - **Program name**—For example, the 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 subject**—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.

- **Event initiator** 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.
- **System info** section:
  - **Host name**—Name of the host on which the file startup prevention was triggered.
  - **Host IP**—IP address of the host on which the file startup prevention was triggered.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user whose account was used to run the file.
  - **OS name**—Version of the operating system being used on the host.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **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.

- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **File**—Name of the blocked document.
  - **MD5**—MD5 hash of the blocked document.
  - **SHA256**—SHA256 hash of the blocked document.
  - **Event time**—Time when the document was blocked.
  - **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.
- **Event initiator** 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.
- **System info** section:
  - **Host name**—Name of the host on which the document was blocked.
  - **Host IP**—IP address of the host on which the document was blocked.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user that attempted to open the document.
  - **OS name**—Version of the operating system being used on the host.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "File modified" event

The window displaying information about **File changed** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- Depending on the type of operation that was performed with the file, one of the following section names is displayed in the event information:
  - **File created**.
  - **File modified**.
  - **File renamed**.
  - **File removed**.
  - **File attributes modified**.
  - **File read**.

  The section displays the following information:

  - **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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **File**—Name of the created, deleted, or modified file.
  - **MD5**—MD5 hash of the created, deleted, or modified file.
  - **SHA256**—SHA256 hash of the created, deleted, or modified file.

- **Size**—Size of the created, deleted, or modified file.
- **Event time**—Time when the event was detected.
- **Time created**—Time when the file was created.
- **Time modified**—Time of last modification of the file.
- **Previous version**—Name of the previous version of the file.

  > The **Previous version** field is displayed in event details only for operations of the **File renamed** type.

- **Remove file after reboot**—Status of the file to be deleted.

  If the file to which the "delete" operation was applied is opened in any program or is used by other processes, it is deleted when these processes terminate after a reboot of the host. In this case, **Remove file after reboot** displays Yes.

  If the file to which the "delete" operation was applied was deleted immediately, the **Remove file after reboot** field displays No.

  > The **Remove file after reboot** field is displayed in event details only for operations of the **File removed** type.

If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the section also includes the following fields:

- **File type**—Extension of the created, deleted, or modified file.
- **File open flags**—Value of the open flags for the created, deleted, or modified file.
- **Owner user name**—Name of the user that created the file.
- **Owner group name**—Name of the group whose users can modify or delete the file.
- **File permitted capabilities**—Permissions that can be used to gain access to a created, deleted, or modified file.
- **File inheritable capabilities**—Permissions that an user group has to perform operations on the parent directory of the created, deleted, or modified file.
- **File effective capabilities**—Permissions that are relevant to the created, deleted, or modified file at the current moment.

- **Event initiator** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **Event initiator** section also includes the following fields:

- **Environment variables**—Environment variables of the process.
- **Real user name**—Name of the user assigned when registering in the system.
- **Real group name**—Group to which the user belongs.
- **Effective user name**—User name that was used to log in to the system.
- **Effective group name**—Group of the user whose name was used to log in to the system.

- **System info** section:
  - **Host name**—Name of the host on which the file was created.
  - **Host IP**—IP address of the host on which the file was created.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user that created the file.
  - **OS name**—Version of the operating system that is being used on the host.

  If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **System info** section also displays the **Logon from remote host** field for the name of host from which the remote logon was performed.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- Copy value to clipboard.

In the information about the event that Kaspersky Endpoint Agent for Linux records in the event database, you can click the links with the file name or file path to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the Get file task.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Agent for Linux records in the event database, you can click the link with the host name to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the following tasks:
  - Get 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 TIP.
- Find in Storage.

- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "System event log" event

The window displaying information about **System event log** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **System event log** 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **Event time**—Time when the event was detected.
  - **Security event ID**—Identifier of the type of security event in the Windows log.

  If the event was logged in the event database by Kaspersky Endpoint Agent for Linux, the **System event log** section also includes the following fields:

  - **Event type**—Type of the event.
  - **Operation result**—For example, **Success** or **Failed**.

- The **Event data** section containing information from the system log. The scope of data depends on the type of Windows event.

  The **Event data** section is not displayed in information about events logged to events database by Kaspersky Endpoint Agent for Linux.

- **Event initiator** section:

  - **File**—Process file name.
  - **Process ID**—Process identifier.
  - **Command**—Command used to run the parent process.
  - **Environment variables**—Environment variables of the process.
  - **Real user name**—Name of the user assigned when registering in the system.
  - **Real group name**—Group to which the user belongs.

  The **Event initiator** section is not displayed in information about events logged to events database by Kaspersky Endpoint Agent for Windows.

- **System info** section:

  - **Host name**—Name of the host on which the event occurred.
  - **Host IP**—IP address of the host on which the event took place.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

  - **User name**—Name of the user who started the process that initiated the system log record.
  - **OS name**—Version of the operating system that is being used on the host.

    Event information logged to events database by Kaspersky Endpoint Agent for Linux also includes the **Logon from remote host** field, that is, the name of the host from which remote logon was performed.

In the information about the event that Kaspersky Endpoint Agent for Linux records in the event database, you can click the links with the file name or file path to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the Get file task.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete file.
  - Quarantine file.
  - Run program.
- **Copy value to clipboard**.

In the information about the event that Kaspersky Endpoint Agent for Linux records in the event database, you can click the link with the host name to open a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Run the following tasks:
  - Get 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **Key path** is the path to the registry key that was modified

- **Value name**: for example, RegistrySizeLimit
- **Value data** is the value of the registry entry
- **Value type**: for example, REG_DWORD
- **Event time** is the time of registry modification

  When changing the name or value of a registry key, you may see additional fields containing information about the state of the registry key prior to its modification:

  - The **Previous key path** field is displayed when the name of the registry key is modified.
  - The **Previous value data** field is displayed when the registry value is modified.
  - The **Previous value type** field is displayed when the type of the registry value is modified.

    Kaspersky Anti Targeted Attack Platform receives the data required to populate the **Previous key path**, **Previous value data**, **Previous value type** fields only when Kaspersky Anti Targeted Attack Platform is integrated with the Kaspersky Endpoint Agent for Windows program version 3.10 or later. When integrating the program with older versions of the Kaspersky Endpoint Agent, the fields are not displayed in the event information.

- **Event initiator** section:
  - **File**—Path to 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.
    - **Copy value to clipboard**.

    Run the following tasks:

    - Kill process.
    - Kill by unique PID.
    - Delete file.
    - Get file.
    - Get forensics.
    - Quarantine file.
  - **MD5**—MD5 hash of the parent process file.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- **Find events**.
- Find alerts.
- Find on TIP.
- Find in Storage.
- Create prevention rule.

Copy value to clipboard.

- **SHA256**—SHA256 hash of the parent process file.
  Clicking the **SHA256** link opens a list in which you can select one of the following actions:
  - **Find events**.
  - Find alerts.
  - Find on TIP.
  - Find in Storage.
  - Create prevention rule.
  - **Copy value to clipboard**.

- **System info** section:
  - **Host name**—Name of the host on which the registry modification was made.
    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**.

    Run the following tasks:
    - **Get data** → File, Forensics, Disk image, Memory dump.
    - Kill process.
    - Delete file.
    - Quarantine file.
    - Run program.
  - **Host IP**—IP address of the host on which the registry modification was made.

If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

- **User name**—Name of the user that made the change in the registry.
- **OS name**—Version of the operating system being used on the host.

You can view information about the modification of the selected register key by editing or replacing the Kaspersky Anti Targeted Attack Platform configuration file. To edit or replace the configuration file of the program, you must contact Technical Support.

You are strongly advised not to perform any operations with the Kaspersky Anti Targeted Attack Platform configuration file in Technical Support Mode without advice or instructions from Technical Support staff.

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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **Local port**—Port that was listened to.
  - **Local IP**—IP address of the network interface whose port was listened to.
  - **Event time**—Port listening time.
- **Event initiator** section:
  - **File**—Path to the parent process file.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.

- **System info** section:
  - **Host name**—Name of the host whose port was listened to.
  - **Host IP**—IP address of the host whose port was listened.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user whose account was used to listen to the port.
  - **OS name**—Version of the operating system that is being used on the host.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create 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.
- Recommendations for processing an event.
- **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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.

- **File**—Name of the loaded driver file.
- **MD5**—MD5 hash of the loaded driver file.
- **SHA256**—SHA256 hash of the loaded driver file.
- **Size**—Size of the loaded driver.
- **Event time**—Time when the driver was loaded.

- **Details** section:
  - **Program name**—For example, the 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 subject**—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**—Time of last modification of the loaded driver.
- **System info** section:
  - **Host name**—Name of the host on which the driver was loaded.
  - **Host IP**—IP address of the host to which the driver was loaded.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—Name of the user that loaded the driver.
  - **OS name**—Version of the operating system being used on the host.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "Alert" event

The window showing information about a **Scan: detect** type event contains the following details:

- Tree of events.
- Recommendations for processing an event.
- On the **Details** tab, in the **Scan: detect** 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **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**.
    - **View on Kaspersky Threats**.
    - **Copy value to clipboard**.
  - **Last action**—Last action taken on the detected object.
  - **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.
  - **Object type**—Type of object (for example, a file).
  - **Detect mode**—Scan mode in which the alert was generated.
  - **Event time**—Date and time of the event.
  - **Record ID**—ID of the record of the alert in the database.

- **Database version**—Version of the database used to generate the alert.
- **Content**—Contents of the script sent to be scanned.

  You can download this data by clicking **Save to file**.

- On the **Details** tab, in the **Event initiator** section:
  - **File**—Path to 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.
    - **Copy value to clipboard**.

    Run the following tasks:

    - Kill process.
    - Kill by unique PID.
    - Delete file.
    - Get file.
    - Get forensics.
    - Quarantine file.
  - **Process ID**—Identifier of the parent process.
  - **Launch parameters**—Parent process startup settings.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.
- On the **Details** tab, in the **System info** section:
  - **Host name**—Name of the host on which the alert was generated.

    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**.

Run the following tasks:

- **Get data** → File, Forensics, Disk image, Memory dump.
- Kill process.
- Delete file.
- Quarantine file.
- Run program.

- **Host IP**—IP address of the host on which the alert was created.

  If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

  The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

- **User name**—User account used to complete the action taken on the detected object.
- **OS name**—Version of the operating system that is being used on the host.

- On the **History** tab, in the table:
  - **Type**—Type of event: **Scan: detect** or **Scan: detect processing result**.
  - **Description**—Description of the event.
  - **Time**—Date and time of detection and alert processing result.

Clicking the **MD5** link opens a list in which you can select one of the following actions:

- Find events.
- Find alerts.
- Find on TIP.
- Find in Storage.
- Create 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 TIP.

- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "Alert processing result" event

The window showing information about a **Scan: detect processing result** type event contains the following details:

- Tree of events.
- Recommendations for processing an event.
- On the **Details** tab, under **Scan: 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **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**.
    - **View on Kaspersky Threats**.
    - **Copy value to clipboard**.
  - **Last action**—Last action taken on the detected object.
  - **MD5**—MD5 hash of the file in which the object was detected.
  - **SHA256**—SHA256 hash of the file in which the object was detected.
  - **Object type**—Type of object (for example, a file).
  - **Object name**—Full name of the file in which the object was detected.
  - **Detect mode**—Scan mode in which the alert was generated.
  - **Event time**—Date and time of the event.
  - **Record ID**—ID of the record of the alert in the database.
  - **Database version**—Version of the database used to generate the alert.

- On the **Details** tab, under **Event initiator**:
  - **File**—Path to the parent process file.
  - **Process ID**—Identifier of the parent process.
  - **Launch parameters**—Parent process startup settings.
  - **MD5**—MD5 hash of the parent process file.
  - **SHA256**—SHA256 hash of the parent process file.
- On the **Details** tab, under **System info**:
  - **Host name**—Name of the host on which the alert was generated.
  - **Host IP**—IP address of the host on which the alert was created.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—User account used to complete the action taken on the detected object.
  - **OS name**—Version of the operating system that is being used on the host.
- On the **History** tab, in the table:
  - **Type** is the type of the **Scan: 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 by unique PID.
  - Delete file.
  - Get file.

    - Get forensics.
    - Quarantine file.
- **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.
- Run the following tasks:
    - **Get data** → File, Forensics, Disk image, Memory dump.
    - Kill process.
    - Delete 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 TIP.
- Find in Storage.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "Interpreted file run" event

The window showing information about **Process: interpreted file run** events contains the following details:

- Tree of events.
- Recommendations for processing an event.
- **Process: 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **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.
- **Event initiator** 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.
- **System info** section:
  - **Host name**—Name of the host on which the file was run.
  - **Host IP**—IP address of the host on which the file was executed.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

- **User name**—Name of the user whose account was used to run the file.
- **OS name**—Version of the operating system being used on the host.

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 by unique PID.
  - Delete file.
  - Get file.
  - Get forensics.
  - Quarantine file.
- **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.
- Run the following tasks:
  - **Get data** → File, Forensics, Disk image, Memory dump.
  - Kill process.
  - Delete 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 TIP.
- Find in Storage.

- Create 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 TIP.
- **Find on virustotal.com**.
- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

Information about the "AMSI scan" event

The window showing information about an **AMSI scan** event contains the following details:

- Tree of events.
- Recommendations for processing an event.
- In the **AMSI scan** 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **Event time**—Date and time of the event.
  - **Content type**—Type of script.

    The program provides two types of scripts:
    - If the script is presented as text, the **Content type** field shows the *Text* script type.
    - If the script is presented in another format, the **Content type** field displays the *Binary* script type.
  - **Content**—Contents of the script sent to be scanned.

    You can copy this data by clicking **Copy to clipboard** if the data is presented as text or download a file containing the data by clicking **Save to file** if the data has a different format.

The **Content** field is displayed in the event information if the program registers signs of targeted attacks.

- In the **Event initiator** section:
  - **File**—Path to 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.
    - **Copy value to clipboard**.

    Run the following tasks:

    - Kill process.
    - Kill by unique PID.
    - Delete file.
    - Get file.
    - Get forensics.
    - Quarantine file.
  - **MD5**—MD5 hash of the parent process file.

    Clicking the **MD5** link opens a list in which you can select one of the following actions:

    - **Find events**.
    - Find alerts.
    - Find on TIP.
    - Find in Storage.
    - Create prevention rule.
    - **Copy value to clipboard**.
  - **SHA256**—SHA256 hash of the parent process file.

    Clicking the **SHA256** link opens a list in which you can select one of the following actions:

    - **Find events**.
    - Find alerts.
    - Find on TIP.

- Find in Storage.
- Create prevention rule.
- **Copy value to clipboard**.

- In the **System info** section:
  - **Host name**—Name of the host on which the alert was generated.

    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**.

    Run the following tasks:
    - **Get data** → File, Forensics, Disk image, Memory dump.
    - Kill process.
    - Delete file.
    - Quarantine file.
    - Run program.
  - **Host IP**—IP address of the host on which the alert was created.

    If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

    The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.
  - **User name**—User account that was used to make the change in the registry.
  - **OS name**—Version of the operating system that is being used on the host.

Information about the "Interactive command input at the console" event

The window showing information about **Process: console interactive input** events contains the following details:

- Tree of events.
- Recommendations for processing an event.

- **Process: 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.

    The field is displayed if a TAA (IOA) rule was triggered when the event was created.
  - **Input type**—Type of input of commands that were passed to the console application.

    The program provides two ways to enter commands:
    - If commands were entered by the user in the console application, the **Input type** field displays the *Console* command input type.
    - If commands were passed to the console application from another application through a pipe, the **Input type** field displays the *Pipe* command input type.

    > Kaspersky Anti Targeted Attack Platform receives the data required to populate the **Input** field only when Kaspersky Anti Targeted Attack Platform is integrated with the Kaspersky Endpoint Agent for Windows program version 3.10. When integrating the program with older versions of the Kaspersky Endpoint Agent program, the field is not displayed in the event information.

    - **Input text**—Text entered at the command line (for example, CMD) on the host with the Kaspersky Endpoint Agent for Windows program.

    You can copy this text by clicking the **Copy to clipboard** button located in the **Input text** field.
  - **Event time**—Time when the event was detected.
- **Event initiator** section:
  - **File**—Path to 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.
    - **Copy value to clipboard**.

    Run the following tasks:
    - Kill process.
    - Kill by unique PID.
    - Delete file.
    - Get file.

- Get forensics.
- Quarantine file.

- **MD5**—MD5 hash of the parent process file.
  Clicking the **MD5** link opens a list in which you can select one of the following actions:
  - **Find events**.
  - Find alerts.
  - Find on TIP.
  - Find in Storage.
  - Create prevention rule.
  - **Copy value to clipboard**.
- **SHA256**—SHA256 hash of the parent process file.
  Clicking the **SHA256** link opens a list in which you can select one of the following actions:
  - **Find events**.
  - Find alerts.
  - Find on TIP.
  - Find in Storage.
  - Create prevention rule.
  - **Copy value to clipboard**.

- **System info** section:
  - **Host name**—Name of the host on which the command was entered.
    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**.

    Run the following tasks:
    - **Get data** → File, Forensics, Disk image, Memory dump.
    - Kill process.
    - Delete file.

- Quarantine file.
- Run program.

- **Host IP**—IP address of the host on which the command was entered.

  If you are using dynamic IP addresses, the field displays the IP address assigned to the host at the moment when the event was created.

  The program does not support IPv6. If you are using IPv6, the IP address of the host is not displayed.

- **User name**—User account that was used to enter the command.
- **OS name**—Version of the operating system that is being used on the host.

Managing Kaspersky Endpoint Agent host information

Kaspersky Endpoint Agent is installed on individual computers (hereinafter also referred to as "hosts") in the IT infrastructure of the organization. The program continuously monitors processes running on those hosts, active network connections, and files that are being modified.

Users with the **Senior security officer**, **Security officer**, **Security auditor**, **Local administrator**, or **Administrator** role 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 tenants to whose data the user has access. If you are using the distributed solution and multitenancy mode, the web interface of the PCN server displays the list of hosts with Kaspersky Endpoint Agent program 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 tenants to whose data they have 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 tenants to whose data the user has 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 staff 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, and other resources) and inform you about the scope of data obtained for debugging purposes. The retrieved diagnostic information 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 this manual 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 Kaspersky Endpoint Agent hosts is located in the **Endpoint Agents** section of the program web interface window.

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**— Name of the server to which the Kaspersky Endpoint Agent host is connected.
- **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:

- **Add to filter**.
- **Exclude from filter**.

- Run the following tasks:
  - Kill process.
  - Delete file.
  - Kill by unique PID.
  - Get file.
  - Get forensics.
  - Quarantine file.
  - Run program.
- New prevention rule.
- Isolate from network.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

> The list of available actions depends on the Kaspersky Endpoint Agent type (for Windows or Linux), version, and activity indicator.

Clicking the link with the IP opens a list in which you can select one of the following actions:

- **Add to filter**.
- **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:

- **Add to filter**.
- **Exclude from filter**.
- **Copy value to clipboard**.

Configuring the display of the table of hosts with the Endpoint Agent component

You can show or hide columns and change the order of columns in the table of hosts with the Endpoint Agent component.

To configure the display of the table of hosts with the Endpoint Agent component:

1. Select the **Assets** section in the application web interface window.
2. Go to the **Endpoint Agents** tab.
3. In the heading part of the table, click .
4. This opens the **Customize table** window.
5. If you want to show a column in the table, select the check box next to the name of the parameter that you want displayed in the table.

   If you want to hide a parameter in the table, clear the check box.

   > At least one check box must be selected.

6. If you want to change the order of columns in the table, move the mouse cursor to the row with the relevant parameter, click and move the row to its new place.
7. If you want to restore default table display settings, click **Default**.
8. Click **Apply**.

The display of the table of hosts with the Endpoint Agent component is configured.

Viewing information about a host

To view information about a Kaspersky Endpoint Agent host:

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 **Blocked application (prevention rule)** event type.

  The **Events affected by prevention rules** link is not displayed in the information for hosts with Kaspersky Endpoint Agent for Linux.

- On the **Details** tab, the **Host** section displays the following information:
  - **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.
- On the **Details** tab, the **Endpoint Agent** section displays the following information:
  - **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.
- **Server**—Name of the SCN or PCN server. Only displayed in distributed solution and multitenancy mode.
- **Connected to server**—Name of the Central Node server.
- **Last connection**—time of the last connection to the Central Node, SCN, or PCN server.
- **License key status**—For example, "OK".
- On the **Prevention rules** tab, 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 **Prevention rules** tab is not displayed in the information for hosts with Kaspersky Endpoint Agent for Linux.

- On the Tasks tab, 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.
  - Get forensics.
  - Quarantine file.
  - Run program.
- New prevention rule.
- Isolate from network.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

For hosts with Kaspersky Endpoint Agent for Linux, the list displayed by clicking the link with the host name includes only **Get file**, **Run program**, **Find events**, and **Find alerts**.

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**.

Filtering and searching hosts with Kaspersky Endpoint Agent by host name

To filter or search for Kaspersky Endpoint Agent hosts 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 Kaspersky Endpoint Agent hosts 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 the 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 Kaspersky Endpoint Agent hosts 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 Kaspersky Endpoint Agent hosts by IP address:

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 Kaspersky Endpoint Agent hosts by operating system version:

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 settings 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 Kaspersky Endpoint Agent hosts by Kaspersky Endpoint Agent version:

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 settings 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 Kaspersky Endpoint Agent hosts 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:

   - **Add to filter**, 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 the Kaspersky Endpoint Agent host filter for one or more filtering criteria:

1. Select the **Endpoint Agents** section in the window of the program web interface.
2. Click to 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. Users with the **Security auditor** role can view the settings of activity indicators of Kaspersky Endpoint Agent. Users with the **Senior security officer** or **Security officer** role 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.

To configure activity indicators for Kaspersky Endpoint Agent program:

1. Sign in to the program web interface under the **Local administrator**, **Administrator** or **Senior security officer** account.
2. In the window of the program web interface, select the **Settings** section, **Endpoint Agents** subsection.
3. In the fields under the section name, enter the number of days of inactivity of hosts with Kaspersky Endpoint Agent that you want to display as **Warning** and **Critical inactivity**.
4. Click **Apply**.

Activity indicators of Kaspersky Endpoint Agent will be configured.

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 doc dot docm docx dotx dotm docb

Process	File extensions
excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
acrord32.exe	pdf
wordpad.exe	docx pdf
chrome.exe	pdf
MicrosoftEdge.exe	pdf

Network isolation of 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 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.

Network isolation is available for hosts with Kaspersky Endpoint Agent version 3.8 or newer.

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.

Keep in mind several limitations when applying network isolation.

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 after** field, enter the time in hours (1 to 9999) during which network isolation of the host will be active.

5. In the **Exclusions for 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.

   You can use a proxy server to let Kaspersky Endpoint Agent for Windows connect to Kaspersky Anti Targeted Attack Platform. When you add this proxy server to exclusions, network resources that can be accessed through the proxy server are also added to exclusions. If network resources that are accessed through the proxy server are added to exclusions, but the proxy server itself is not, such exclusions do not work.

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** 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.

Users with the **Security auditor** and **Security officer** roles cannot create network isolation rules.

The network isolation feature is not available for hosts with Kaspersky Endpoint Agent for Linux.

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 exclusions** link to expand the **Exclusions for the host isolation rule** settings group.
4. Select the direction of network traffic that must not be blocked:

   - **Incoming/Outgoing**.
   - **Incoming**.
   - **Outgoing**.

5. In the **IP** field, enter the IP address whose network traffic must not be blocked.

6. If you selected **Incoming** or **Outgoing**, in the **Ports** field, enter the connection ports.

7. If you want to add more than one exclusion, click **Add** and repeat the steps to fill in the **Traffic direction**, **IP** and **Ports** fields. Click **Save**.

The network isolation rule exclusion will be added.

You can use a proxy server to let Kaspersky Endpoint Agent for Windows connect to Kaspersky Anti Targeted Attack Platform. When you add this proxy server to exclusions, network resources that can be accessed through the proxy server are also added to exclusions. If network resources that are accessed through the proxy server are added to exclusions, but the proxy server itself is not, such exclusions do not work.

Users with the **Security auditor** and **Security officer** roles cannot create exclusions from a network isolation rule.

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.

Users with the **Security auditor** and **Security officer** roles cannot remove network isolation rules.

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 application 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 application 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.

Automatically sending files from Kaspersky Endpoint Agent hosts to be scanned by the Sandbox component in accordance with Kaspersky TAA (IOA) rules

If this functionality is enabled, the application can automatically send files from hosts with the Endpoint Agent component for scanning with the Sandbox component in accordance with Kaspersky TAA (IOA) rules. Files are sent in accordance with the following principle:

1. Kaspersky Anti Targeted Attack Platform checks the event database and marks events that match TAA (IOA) rules.
2. If relevant conditions are found in TAA (IOA) rules, Kaspersky Anti Targeted Attack Platform sends files for scanning by the Sandbox component.

   > Requests for scanning files by the Sandbox component are not displayed in the Kaspersky Anti Targeted Attack Platform web interface.

3. Based on the results of the scan, the application may create an alert.

   You can view alerts created in this way by filtering alerts by the **Details** – **Autosend to Sandbox** attribute.

If automatic sending of files to be scanned by the Sandbox component is enabled, the volume of traffic processed by the component can become very large. If the Sandbox component server cannot support the increased load, some of the objects from the processing request queue are replaced with requests for processing files that are automatically sent for scanning.

To avoid dropping objects from the processing request queue, you can:

- Deploy additional Sandbox servers.
- Disable automatically sending files to be scanned by the Sandbox component.

- Add to exclusions those TAA (IOA) rules that most frequently cause Kaspersky Anti Targeted Attack Platform to send files for scanning by the Sandbox component.

  Information about rules that are most frequently used by Kaspersky Anti Targeted Attack Platform to send files for scanning by the Sandbox component is displayed in the **Sent to Sandbox by TAA rules** widget. You can add this widget to your current layout.

  When you add a file to exclusions, event marking and creation of alerts in accordance with this rule is also stopped.

Files that can be automatically sent for scanning by the Sandbox component are listed in the following table.

List of files that can be automatically sent for scanning by the Sandbox component

Event type	File type
Process started	File of the started process and file of its parent process.
Module loaded	File of the loaded module and file of its parent process.
Connection to remote host	File of the parent process.
Blocked application (prevention rule)	File of the application that was blocked from running, and file of its parent process.
Document blocked	File of the document that was blocked from running, and file of its parent process.
File changed	Created, deleted, or modified file and file of the parent process.
System event log	File of the process (only for Linux).
Registry modified	File of the parent process.
Port listened	File of the parent process.
Driver loaded	File of the loaded driver.
Detection	Detected file and file of its parent process (if any).
Detection processing result	Detected file and file of its parent process (if any).
AMSI scan	File of the process.
Process: interpreted file run	File that was started and file of its parent process.
Process: console interactive input	File of the parent process.

Information about files sent for scanning by the Sandbox component is not displayed in the Kaspersky Anti Targeted Attack Platform web interface.

Enabling and disabling the automatic sending of files from Kaspersky Endpoint Agent hosts to be scanned by the Sandbox component

To enable or disable automatically sending files to be scanned by the Sandbox component in accordance with Kaspersky TAA (IOA) rules:

1. In the window of the program web interface, select the **Settings** section, **Endpoint Agents** subsection.
2. Under **Send files to Sandbox automatically**:
   - Select the **Send files** check box if you want files to be sent automatically.

     This function is enabled by default.
   - Clear the **Send files** check box if you do not want files to be sent automatically.

     Disabling this functionality does not affect the functioning of TAA (IOA) rules; only automatic sending of files is disabled.
3. Click **Apply**.

Automatically sending files to be scanned by the Sandbox component in accordance with Kaspersky TAA (IOA) rules is enabled or disabled.

In distributed solution and multitenancy mode, settings for automatically sending files for scanning by the Sandbox component in accordance with Kaspersky TAA (IOA) rules configured on the PCN server are also applied on SCN servers connected to that PCN server. If necessary, you can enable or disable the automatic sending of files on each selected SCN server individually.

Managing tasks

In the web interface of the program, users with the **Senior security officer** role can manage files and programs on hosts by creating and removing tasks.

In distributed solution and multitenancy mode, **Kill process**, **Get forensics**, **Get registry key**, **Start YARA scan**, **Service management**, **Run program**, **Delete file**, **Restore file from quarantine**, **Quarantine file** tasks can have 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 tenant for which the user is managing the program using the 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 tenant for which the user is managing the program using the web interface.

The tasks **Get file**, **Get process memory dump**, **Get NTFS metafiles**, **Get disk image**, **Get memory dump** run only on the specified host, regardless of the program operating mode.

The maximum task execution time is 24 hours. If the task did not complete in this time, execution is paused.

Users with the **Senior security officer** role can manage all tasks for tenants to whose data they have access.

Users with the **Security officer** role do not have access to tasks.

Users with the **Security auditor** role can view the task table and information about the selected task.

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).

You can show or hide tasks created by you using the **Only mine** toggle 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:

- **Time**—Task creation date and time.
- **Type** is the type of the task depending on the operating mode of the program and the server on which the task was created.

  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 tenant for which the user is managing the program using the 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 tenant for which the user is managing the program using the web interface.
- **Name**—Task name.

  A task can have one of the following names:

  - **Kill process**.
  - **Get forensics**.
  - **Start YARA scan**.
  - **Service management**.
  - **Get NTFS metafiles**.
  - **Get registry key**.
  - **Get process memory dump**.
  - **Run program**.
  - **Get file**.
  - **Delete file**.

- **Quarantine file**.
- **Restore file from quarantine**.
- **Get disk image**.
- **Get memory dump**.

Clicking the link with the name of the task type opens a list in which you can select one of the following actions:

- **Add to filter**.
- **Exclude from filter**.
- **Copy value to clipboard**.

- **Details**—full path to the file or data stream for which the task was created, or the path to a shared network resource.

  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:

  - **Add to filter**.
  - **Exclude from filter**.
  - **Copy value to clipboard**.

- **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 the distributed solution and multitenancy mode.

- **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.

- **Created by**—Name of the user who created the task.

  > If only tasks created by the current user are displayed, this column is not displayed.

- **State**—Task completion status.

  A task can have one of the following statuses:

  - **Pending**.
  - **In process**.
  - **Completed**.

Viewing information about a task

To view task details:

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.
- **Information type**—Type of the collected data.
- **Registry key**—Path to the registry key that you want to get.
- **Process ID**—Process identifier.
- **File mask**—Mask of files that are included in the data list.
- **Metafiles**—NTFS metafiles that you want to get.
- **Volume**—Name of the drive from which you want to receive metafiles, disk image, or memory dump.
- **Share path**—Path to a shared network resource.
- **Stored file**—Link to the file received as a result of the task execution.
- **Maximum nesting level**—Maximum nesting level of folders which the program searches for files.
- **Exclusions**—Folders in which searching and scanning files is prohibited.
- **Scan scope**—Folders which are scanned by YARA rules.
- **Action**—Action that was performed for the service.
  The program supports the following operations with services:
  - **Start**.
  - **Stop**.
  - **Pause**.
  - **Resume**.

- **Delete**.
- **Modify startup type**.

- **Maximum scan duration**—Maximum task execution time, after which the scan is stopped.
- **SHA256**—SHA256 hash of the file that you want to receive.
- **Run as**—Option to run the program using the name of the local system.
- **Created by**—Name of the user who created the task.
- **Tenant**—Name of the tenant. Displayed only when you are using the 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 get file task

You can download a file from selected Kaspersky Endpoint Agent for Windows hosts. To do so, you must create a get file task.

The file to be downloaded must not exceed 100 MB. If the file exceeds 100 MB, the task finishes with an error.

To create a get file task:

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click the **Add** button and select **File** in the **Get data** drop-down list.

   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.

   When creating a task, the program does not check if the specified path to the file that you want to receive is valid.

   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** is the name or IP address of the host.

You can specify only one host.

4. Click **Add**.

The get file task will be created. The task runs automatically after it is created.

A file received through this task will be placed in Storage. If the get file task completed successfully, you can download the received file to your local computer.

If you are using the distributed solution and multitenancy mode, the archive is placed in Storage of the Central Node server to which the host specified in the **Host** field is connected.

You can also download the file from the task report window.

To download the file from the task report window:

1. Select the **Tasks** section in the program web interface window.

This opens the task table.

2. Open the get file task that you want to download.

3. In the **Report** section, click the name or IP address of the host.

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.

Users with the **Security auditor** role cannot create get file tasks.

Users with the **Security officer** role do not have access to tasks.

Creating a forensic collection task

You can get lists of files, processes, and autorun points from selected Kaspersky Endpoint Agent for Windows hosts. To do so, you must create a forensic collection task.

To create a forensic collection task:

1. Select the **Tasks** section in the program web interface window.

This opens the task table.

2. Click the **Add** button and select **Forensics** in the **Get data** drop-down list.

   This opens the task creation window.

3. Configure the following settings:

   a. **Information type** is the type of collected data. Select the check box next to one, multiple, or all settings:

   - **Processes list** if you want to get a list of processes running on the host at the time of the task execution.

   - **Autorun points list** if you want to get a list of autorun points.

     The autorun points list includes information about programs added to the startup folder or registered in the Run keys of the registry, as well as programs that are automatically run at startup of a Kaspersky Endpoint Agent host and when a user logs in to the operating system on the specified hosts.

     List of supported autorun points

     Kaspersky Endpoint Agent supports gathering data for the following autorun points:

     - Logon.
     - Run.
     - Explorer.
     - Shell.
     - Office.
     - Internet Explorer®.
     - Tasks.
     - Services.
     - Drivers.
     - Telephony.
     - Cryptography.
     - Debuggers.
     - COM.
     - Session Manager.
     - Network.
     - LSA.
     - Applications.
     - Codecs.
     - Shellex.

- WMI.
- Unspecified.

- **File list** if you want to get a list of files stored in the selected folder or in all host folders at the time of the task execution.

b. If you have selected the **File list** check box, in the **Source type** group of settings, select one of the following options:

- **All local disks** if you want the list of files to include files stored in all folders on local disks at the time of the task execution.
- **Directory** if you want the file list to include files stored in the specified folder and its subfolders at the time when the task is run.

c. If you selected **Directory**, in the **Start directory** field, specify the path to the folder from which the file search should start.

You can use the following prefixes:

- System environment variables.
- User-defined environment variables.

  When using user-defined environment variables, the list of files includes information about files in folders of all users who have set the specified environment variables. If user-defined environment variables override system environment variables, the list of files includes information about files in folders based on the values of system environment variables.

d. In the **Hosts** field, enter the IP address or name of the host to which you want to assign the task.

You can specify multiple hosts.

> The data collection task can only be assigned to hosts with the Kaspersky Endpoint Agent for Windows program version 3.10 or later. Getting a list of autorun points is only supported on hosts with Kaspersky Endpoint Agent for Windows 3.12 or later.

If necessary, you can specify the following search criteria for files in folders:

- **File mask** is the mask of files to be included in the list of files.
- **Alternative data streams** is the check box that enables recording information about alternate data streams in the file list.

  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.

  The check box is selected by default.
- **Maximum nesting level** is the maximum nesting level of folders in which the program searches for files.
- **Exclusions** is the path to the folders in which you want to prohibit the search for information about files.
- **Description** is the task description.

4. Click **Add**.

The forensic collection task is created. The task runs automatically after it is created.

Upon completion of the task, the program places the ZIP-archive which contains file with the selected data into the Storage. If the task completed successfully, you can download the archive to your local computer.

Users with the **Security auditor** role cannot create forensic collection tasks.

Users with the **Security officer** role do not have access to tasks.

Creating a registry key retrieval task

You can get a registry key from selected Kaspersky Endpoint Agent for Windows hosts. To do so, you must create a registry key retrieval task.

To create a registry key retrieval task:

1. Select the **Tasks** section in the program web interface window.
   This opens the task table.
2. Click the **Add** button and select **Registry key** in the **Get data** drop-down list.
   This opens the task creation window.
3. Configure the following settings:
   a. **Registry key** is the registry key that you want to get.
      You can enter the registry key in one of the following formats:
      - Relative to the root key.
        For example, \REGISTRY\MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.
      - Relative with full name of the root key.
        For example, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.
      - Relative with an abbreviation instead of the full name of the root key.
        For example, HKLM\SOFTWARE\Microsoft\WindowsUpdate\Orchestrator.

      If you want to get data from HKEY_CURRENT_USER, you must specify HKEY_USERS and the SID of the user: HKEY_USERS\<SID of the user>.

   b. **Description**—Task description. This field is optional.
   c. In the **Hosts** field, enter the name or IP address of the host to which you want to assign the task.
      You can specify multiple hosts.

The registry key retrieval task can only be assigned to hosts with the Kaspersky Endpoint Agent for Windows program version 3.13 or later.

4. Click **Add**.

   The registry key retrieval task is created. The task runs automatically after it is created.

As a result of the task, the program places a ZIP archive in Storage; the archive contains a .reg file, which contains a list of all registry keys and values under the key that was specified when creating the task. You can download the archive to your local computer.

If the task results in an error, the archive file contains the description of the error.

Users with the **Security auditor** role cannot create this task.

Users with the **Security officer** role do not have access to tasks.

Creating an NTFS metafile retrieval task

You can get NTFS metafiles from selected Kaspersky Endpoint Agent for Windows hosts. To do so, you must create an NTFS metafile retrieval task.

To create an NTFS metafile retrieval task:

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click the **Add** button and select **NTFS metafiles** in the **Get data** drop-down list.

   This opens the task creation window.

3. Configure the following settings:

   a. **Metafiles** is the list of metafiles that you can get using the task. Select the relevant metafile by selecting the corresponding check box.

      You can select multiple metafiles.

   b. **Volume** is the name of the disk from which you want to get metafiles.

      By default, the system disk is specified. You can enter the path to a different disk in the `<drive letter>:` format.

   c. **Description**—Task description. This field is optional.

   d. **Host**is the name or IP address of the host to which you want to assign the task.

      You can specify only one host.

The NTFS metafile retrieval task can only be assigned to hosts with the Kaspersky Endpoint Agent for Windows program version 3.13 or later.

4. Click **Add**.

   The NTFS metafile creation task is created. The task runs automatically after it is created.

When the task finishes, the program places a ZIP archive containing the selected metafiles in Storage. You can download the archive to your local computer.

If the task results in an error, the archive file contains the description of the error.

If you are using the distributed solution and multitenancy mode, the archive is placed in Storage of the Central Node server to which the host specified in the **Host** field is connected.

If downloading selected metafiles exhausts Storage capacity, objects in Storage will be rotated. If a metafile is larger than total Storage capacity, it is not downloaded

Users with the **Security auditor** role cannot create this task. Users with the **Security officer** role do not have access to tasks.

Creating a process memory dump retrieval task

You can get a process memory dump file from the selected Kaspersky Endpoint Agent for Windows hosts. To do so, you must create a process memory dump retrieval task.

To create a process memory dump retrieval task:

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click the **Add** button and select **Process memory dump** in the **Get data** drop-down list.

   This opens the task creation window.

3. Configure the following settings:

   a. **Process ID** is the ID of the process for which you want to get a memory dump.

   b. **MD5/SHA256** is the MD5 or SHA256 hash of the file of the process of which you want to get a memory dump. This field is optional.

   c. **Description**—Task description. This field is optional.

   d. **Host**is the name or IP address of the host to which you want to assign the task.

      You can specify only one host.

The process memory dump task can only be assigned to hosts with Kaspersky Endpoint Agent for Windows version 3.13 or later.

4. Click **Add**.

   The process memory dump retrieval task is created. The task runs automatically after it is created.

The task creates a ZIP archive in Storage, which contains a file with information about the process and a process memory dump file. You can download the archive to your local computer.

If the task results in an error, the archive file contains the description of the error.

If you are using the distributed solution and multitenancy mode, the archive is placed in Storage of the Central Node server to which the host specified in the **Host** field is connected.

Users with the **Security auditor** role cannot create this task.

Users with the **Security officer** role do not have access to tasks.

Creating a disk image retrieval task

You can retrieve a disk image from selected Kaspersky Endpoint Agent for Windows host. To do so, you must create an NTFS disk image retrieval task.

The resulting file can be saved only to a shared network resource.

To create a disk image retrieval task:

1. Select the **Tasks** section in the application web interface window.

   This opens the task table.

2. Click the **Add** button and select **Disk image** in the **Get data** drop-down list.

   This opens the task creation window.

3. Configure the following settings:

   a. **Share path**—path to a shared network resource.

      You need to specify the path in the Universal Naming Convention (UNC) format: `\\server\share\path`.

   b. **User name**—user name of the account used to access the shared network resource.

   c. **Password**—password of the account used to access the shared network resource.

   d. Under **Disk type**, select one of the following options:

      - **Logical**.
      - **Physical**.

e. If you selected **Logical**, enter a `%SystemDrive%` variable or a drive letter without the colon and slash in the **Volume** field.

f. If you selected **Physical**, enter the disk number in the **Physical drive** field.

g. Select the **Split file into parts** check box if you want the file to be divided into multiple parts when saved.

h. If you selected the check box, in the **Part size, GB** field, specify the minimum size of one part of the saved file.

The minimum part size must be more than one gigabyte.

i. **Description** is the task description. This field is optional.

j. **Host**—the IP address or name of the host to which you want to assign the task.

4. Click **Add**.

The disk image retrieval task will be created. The task runs automatically after it is created.

The application places an archive containing a file or files in the EWF or RAW format in a network share. You can convert files from the RAW format to the EWF format.

Users with the **Security auditor** role cannot create tasks.

Users with the **Security officer** role do not have access to tasks.

Creating a RAM dump retrieval task

You can retrieve a RAM dump from a selected host with the Endpoint Agent component. To do so, you must create a memory dump retrieval task.

The resulting file can be saved only to a shared network resource.

To create a memory dump retrieval task:

1. Select the **Tasks** section in the application web interface window.

This opens the task table.

2. Click the **Add** button and select **Memory dump** in the **Get data** drop-down list.

This opens the task creation window.

3. Configure the following settings:

a. **Share path**—path to a shared network resource.

You need to specify the path in the Universal Naming Convention (UNC) format: `\\server\share\path`.

b. **User name**—user name of the account used to access the shared network resource.

c. **Password**—password of the account used to access the shared network resource.

d. **Description** is the task description. This field is optional.

e. **Host**—the IP address or name of the host to which you want to assign the task.

4. Click **Add**.

The RAM dump retrieval task is created. The task runs automatically after it is created.

As a result, the application places a RAW file or an archive that contains a RAW file on the shared network resource.

Users with the **Security auditor** role cannot create tasks.

Users with the **Security officer** role do not have access to tasks.

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 **Add** 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. **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 **Add**.

The process termination task will be created. The task runs automatically after it is created.

Users with the **Security auditor** role cannot create process termination tasks.

Users with the **Security officer** role do not have access to tasks.

Creating a task to scan hosts using YARA rules

You can scan Kaspersky Endpoint Agent for Windows hosts using YARA rules. To do so, you must create a **Start YARA scan** task. You can create the task:

- In the **Tasks** section.

  In this case, when creating the task, you must select YARA rules that you want to use to scan hosts.
- In the **Custom rules** section, **YARA** subsection.

  In this case, a task is created to scan hosts using selected YARA rules.

*To create a task for scanning Kaspersky Endpoint Agent for Windows hosts using YARA rules in the **Tasks** section:*

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.
2. Click **Add** and select **Start YARA scan**.

   This opens the task creation window.
3. Configure the following settings:

   a. **Select rules** is the name of the rule. You can enter the name of the rule or a sequence of characters from the name of the rule, then select the rule in the list.

   You can add multiple rules.

b. **Scan** is the scan scope. Select one of the following options:

- **RAM** if you want to scan processes that are running at the time of the task execution.

  The program does not scan processes with a low priority.

- **Autorun points** if you want to scan autorun points obtained from the **Get forensics** task.

  Only available when integrated with Kaspersky Endpoint Agent 3.13 or later.

  To have autorun points scanned, you must specify hosts for which the **Get forensics** was previously run.

- **Specified directories** if you want to scan files that are located in a specified folder and all its nested folders at the time of the task execution.

- **All local disks** if you want to scan files stored in all folders on local disks at the time of the task execution.

  Scanning all local disks can cause high load on the host.

c. If you selected **RAM**, if necessary, do the following:

- In the **Processes** field, enter short names of processes or a mask of files that you want to scan.

  The program scans all processes with identical names that are running on the host.

  If the **Processes** field is left blank, the program scans all processes that were running at the time of the task execution, except processes with PID under 10 and processes listed in the **Exclusions** field.

- In the **Exclusions** field, enter short names of processes or a mask of files that you want to exclude from scanning.

  If multiple processes with identical names are running on the host, the program excludes all such processes from scanning.

d. If you selected **Autorun points**, in the **Scan type** field, select the scan type:

- **Quick**.

  In this case, all autorun points are scanned, except COM objects.

- **Full**.

  In this case, all autorun points are scanned, as well as files involved with them.

e. If you selected **Specified directories**:

- In the **Specified directories** field, enter the full path to folders, name or mask of files that you want to scan (for example, C:\Users\User1\Documents* or C:\Program files*.exe).

- In the **Exclusions** field, enter the full path to folders, name or mask of files that you want to exclude from scanning.

f. **Maximum scan duration** is the maximum scan duration.

When this time elapses, the scan is stopped even if some rules were not applied to scan the hosts. The task report contains results that are up-to-date at the moment when the scan was stopped.

g. **Description**—Task description. This field is optional.

h. **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.

  The task of scanning Kaspersky Endpoint Agent hosts by YARA rules can only be assigned to hosts with Kaspersky Endpoint Agent for Windows 3.12 or later. If you simultaneously assign a task to hosts with Kaspersky Endpoint Agent 3.12 and earlier versions of the program, the task is executed only on hosts with Kaspersky Endpoint Agent 3.12.

*To create a task for scanning Kaspersky Endpoint Agent for Windows hosts using YARA rules in the **Custom rules** section, **YARA** subsection:*

1. In the window of the program web interface, select the **Custom rules** section, **YARA** subsection.
2. Select check boxes to the left of rules that you want to use when scanning the hosts.

   A control panel appears in the lower part of the window.
3. Click **Start YARA scan**.
4. Carry out step 3 of the instruction above.

Task creation is complete. The task runs automatically after it is created.

If the scan detects any threats, Kaspersky Anti Targeted Attack Platform creates corresponding alerts.

Users with the **Security auditor** role cannot create a task to scan Kaspersky Endpoint Agent for Windows hosts by YARA rules.

Users with the **Security officer** role do not have access to tasks.

Creating a service management task

You can remotely start, stop, pause, or resume a service, as well as remove a service or change its start type on selected Kaspersky Endpoint Agent for Windows hosts. To do so, you must create a service management task.

To create a service management task:

1. Select the **Tasks** section in the program web interface window.

   This opens the task table.

2. Click **Add** and select **Service management**.

   This opens the task creation window.

3. Configure the following settings:

   a. In the **Service name** field, enter the name of the service.

   b. In the **MD5/SHA256** field, enter the MD5 or SHA256 hash of the service. This field is optional.

   If you enter the hash of a service that is loaded from a DLL, Kaspersky Anti Targeted Attack Platform simultaneously compares the specified hash with the hash of the service DLL and the hash of the svchost process.

   c. In the **Action** field, select the operation that you want to perform on the service.

   The program supports the following operations with services:

   - **Start**.
   - **Stop**.
   - **Pause**.
   - **Resume**.
   - **Delete**.
   - **Modify startup type**.

   When you remove a service, processes that the service has started keep running until the system is restarted or the process is terminated.

   d. If you selected **Modify startup type**, in the **Startup type**, select the start type for the service.

   e. **Description** is the task description. This field is optional.

   f. **Task for**—Task scope:

   - If you want to run the task on all hosts of all servers, select the **All hosts** option.
   - If you want to run the task on selected servers, select the **Specified servers** option and on the right of the **Servers** parameter name select the check boxes next to the names of the servers on which you want to run the task.

     This option is available only when distributed solution and multitenancy mode is enabled.

   - If you want to run the task on selected hosts, select the **Specified hosts** option and list these hosts in the **Hosts** field.

You can assign the task only to hosts with Kaspersky Endpoint Agent for Windows 3.12 or later. Host with earlier versions of Kaspersky Endpoint Agent for Windows and Kaspersky Endpoint Agent for Linux hosts are displayed in the list of hosts but cannot be selected.

4. Click **Add**.

The service management task is created. The task runs automatically after it is created.

Stopping, pausing, deleting services or changing the start type of services that affect the functioning on the host is strongly discouraged.

List of services for which management is not recommended

- AVP*.
- BFE.
- CertPropSvc.
- CoreMessagingRegistrar.
- CryptSvc.
- DcomLaunch.
- Dhcp.
- DispBrokerDesktopSvc.
- EventLog.
- EventSystem.
- LanmanServer.
- LanmanWorkstation.
- LSM.
- mpssvc.
- Netlogon.
- Netman.
- PlugPlay.
- PolicyAgent.
- Power.
- ProfSvc.
- RasMan.
- RpcEptMapper.
- RpcSs.
- SamSs.
- SCardSvr.
- SecurityHealthService.
- SessionEnv.
- Spooler.
- SstpSvc.
- TermService.
- UmRdpService.
- UserManager.
- UsoSvc.
- VaultSvc.
- W32Time.
- WebClient.
- Winmgmt.
- WlanSvc.
- wscsvc.

Users with the **Security auditor** role cannot create service management tasks.

Users with the **Security officer** role do not have access to tasks.

Creating a program execution task

You can create 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 **Add** 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.

     When creating a task, the program does not check if the specified path to the executable file is valid.

   - 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 working directory (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 **Add**.

The program startup task or command execution task will be created. The task runs automatically after it is 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 **Add** 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 **Add**.

Users with the **Security auditor** role cannot create program running tasks or command execution tasks.

Users with the **Security officer** role do not have access to tasks.

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 **Add** 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 **Add**.

The file deletion task will be created. The task runs automatically after it is created.

If the file has been blocked by another process, the task will be displayed with the *Completed* status but the file will be deleted only after the host is restarted. It is recommended to check whether the file is successfully deleted after the host is restarted.

Deleting the file from a mapped network drive is not supported.

Users with the **Security auditor** role cannot create file deletion tasks.

Users with the **Security officer** role do not have access to tasks.

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 **Add** 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 quarantine.

   b. In the **MD5/SHA256** field, enter the MD5 or SHA256 hash of the file that you want to quarantine. This field is optional.

   c. **Description**—Task description. This field is optional.

   d. In the **Hosts** field, enter the name or IP address of the host to which you want to assign the task.

   You can specify multiple hosts.

   e. Click **Add**.

The file quarantine task is created. The task runs automatically after it 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.

Users with the **Security auditor** role cannot create file quarantine tasks.

Users with the **Security officer** role do not have access to tasks.

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 **Add** 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 **Add**.

The task for restoring a file from Quarantine is created. The task runs automatically after it is created.

After restoring a file from Quarantine to a host, metadata about the file remains in the table of objects placed in Storage.

Users with the **Security auditor** role cannot create tasks to restore files from Quarantine.

Users with the **Security officer** role do not have access to tasks.

Creating a copy of a task

To copy the 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 **Duplicate**.
   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 **Add**.

A copy of the selected task will be created.

Users with the **Security auditor** role cannot copy tasks.

Users with the **Security officer** role do not have access to tasks.

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 is also 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.

Users with the **Security auditor** role cannot delete tasks.

Users with the **Security officer** role do not have access to tasks.

Filtering tasks by creation time

To filter tasks by 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 tenant for which the user is managing the program using the 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 tenant for which the user is managing the program using the web interface.

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 forensics**
   - **Start YARA scan**
   - **Service management**
   - **Get file**
   - **Delete file**
   - **Quarantine file**
   - **Restore file**
   - **Get disk image**
   - **Get memory dump**

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 by 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 by 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 by 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 the status of their processing by the user:

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 the task filter for one or more filtering criteria:

1. Select the **Tasks** section in the program web interface window.
   This opens the task table.
2. Click to 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, such as **Find events**, **Find alerts**, **Find on TIP**, or **Find on virustotal.com**.

In distributed solution and multitenancy mode, 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 tenant which the user is managing 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 tenant which the user is managing in the program web interface.

Users with the **Senior security officer** role can create, edit, delete, enable, disable, and import prevention rules for tenants to whose data they have access.

Users with the **Security officer** role do not have access to policies.

Users with the **Security auditor** role can view the table of file run prevention rules and process run prevention rules, as well as information about the selected prevention rule, but they cannot edit the 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 or imported prevention rules as for manually created rules.

You can create only one prevention rule for each file hash.

The maximum supported number of prevention rules in the system is 50,000.

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.

You can manage file and process running prevention rules on selected hosts using policies if Kaspersky Endpoint Agent is integrated with the Central Node server; to do so, you must use the web interface of Kaspersky Anti Targeted Attack Platform.

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** is the type of the rule depending on the program operating mode and the role of the server on which the rule was created:

   - **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 tenant which the user is managing 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 tenant which the user is managing in the program web interface.

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 the 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:

   - **Add to filter**.

   - **Exclude from filter**.

   - **Find on 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**
   - **Disabled**

Configuring prevention rule table display

You can show or hide columns and change the order of columns in the prevention rule table.

To configure prevention rule table display:

1. Select the **Prevention** section in the application web interface window.

   This opens the prevention rule table

2. In the heading part of the table, click  .

   This opens the **Customize table** window.

3. If you want to show a column in the table, select the check box next to the name of the parameter that you want displayed in the table.

   If you want to hide a parameter in the table, clear the check box.

   > At least one check box must be selected.

4. If you want to change the order of columns in the table, move the mouse cursor to the row with the relevant parameter, click  and move the row to its new place.

5. If you want to restore default table display settings, click **Default**.

6. Click **Apply**.

The prevention rule table display is configured.

Viewing a prevention rule

To view 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**
  - **Disabled**
- 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 TIP**.
    - **Find events**.
    - **Find alerts**.
    - **Copy value to clipboard**.
  - **Name** is the name of the prevention rule or file prevented from running.
  - **Type** is the type of the rule depending on the program operating mode and the role of the server on which the rule was created:
    - **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 tenant which the user is managing 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 tenant which the user is managing in the program web interface.
  - **Notification** is the state of the **Notify user about blocking file 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 **Add**.

3. Select **Create rule**.

   This opens the prevention rule creation window.

4. 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 display a notification about prevention rule triggering to the user of the computer on which the prevention is applied, select the **Notify user about blocking file execution** check box.

   > If you selected the **Notify user about blocking file execution** check box and an attempt is made to execute a file prevented from running, the user is notified that an execution prevention rule was triggered by this file.

   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.

Prevention rules cannot be created for hosts with the Kaspersky Endpoint Agent for Linux program. When creating a prevention rule, if you select a host with Kaspersky Endpoint Agent for Linux or all hosts as the scope of the rule, the rule is not applied or is only applied to hosts with Kaspersky Endpoint Agent for Windows.

5. Click **Add**.

   The file startup prevention will be created.

You can also import prevention rules.

Users with the **Security auditor** role cannot create file launch prevention rules.

Users with the **Security officer** role cannot access prevention rules.

Importing prevention rules

You can import a file with MD5 and SHA256 hashes for files that you want to prevent from running. For each hash, Kaspersky Anti Targeted Attack Platform creates a separate prevention rule.

The maximum size of the imported file is 10 MB. Only one hash per line is allowed.

To import prevention rules:

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table.

2. Click **Add**.

3. Select **Import rules**.

   This opens the prevention rule import window.

4. Configure the following settings:

   a. **State** is the state of the prevention rule:

   - If you want to enable all imported prevention rules, set the toggle switch to **On**.
   - If you want to disable all imported prevention rules, set the toggle switch to **Off**.

   b. If you want the program to display a notification about prevention rules triggering to the user of the computer on which the prevention is applied, select the **Notify user about blocking file execution** check box.

The **Prevent on** field cannot be edited. By default, prevention rules created on a PCN server are applied on all hosts connected to that PCN server and all SCN servers connected to that PCN server (if you are using the distributed solution and multitenancy mode).

5. Click **Browse** to upload the file containing hashes of files for which you want to create prevention rules.

   This opens the file selection window.

6. Select the file that you want to upload and click **Open**.

   This closes the file selection window.

7. Click **Add**.

The rules are imported.

Users with the **Security auditor** role cannot import file launch prevention rules.

Users with the **Security officer** role cannot access prevention rules.

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 **Disabled**.

     The prevention rule you selected will be disabled.

Users with the **Security auditor** role cannot enable or disable prevention rules.

Users with the **Security officer** role do not have access to the prevention rules for launching files and processes on selected hosts using policies.

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 **Disabled**.

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 single 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 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 prevention rules are deleted.

Users with the **Security auditor** role cannot delete prevention rules.

Users with the **Security officer** role do not have access to the prevention rules for launching files and processes on selected hosts using policies.

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 filter 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 tenant which the user is managing 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 tenant which the user is managing in the program web interface.

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 the 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 the prevention rule filter for one or more filtering criteria:

1. Select the **Prevention** section in the program web interface window.

   This opens the prevention rule table.

2. Click to the right of the header of the column of the prevention rule table 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

You can configure additional security for the IT infrastructure of the company using TAA, IDS, IOC, and YARA rules.

Users with the **Senior security officer** role can work with custom **TAA**, **IDS**, **IOC**, and **YARA** rules: load and delete rule files, view lists of rules, and edit the selected rules.

Users with the **Security auditor** role can view the lists of custom **TAA**, **IDS**, **IOC**, and **YARA** rules and properties of selected rules without the possibility of editing.

Users with the **Security officer** role can view the lists of custom **TAA**, **IOC**, and **YARA** rules and properties of selected rules without the possibility of editing.

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 being 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. 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, this section displays information for the selected tenant.

Managing user-defined IOC rules

You can use IOC files to search indicators of compromise in the event database and on computers with Kaspersky Endpoint Agent installed. For example, if you have received third-party information about a piece of malware spreading, you can:

1. Upload an IOC file containing indicators of compromise corresponding to the malware to Kaspersky Anti Targeted Attack Platform.

2. Find events corresponding to the criteria of the selected IOC file.

   You can view such events, and if you want Kaspersky Anti Targeted Attack Platform to generate alerts for selected events, you can create a TAA (IOA) rule.

3. Enable automatic use of the selected IOC file to search indicators of compromise on Kaspersky Endpoint Agent computers.

   If while scanning the computers, Kaspersky Anti Targeted Attack Platform discovers indicators of compromise, Kaspersky Anti Targeted Attack Platform generates an alert.

4. Configure the schedule for searching for indicators of compromise using IOC files on Kaspersky Endpoint Agent computers.

In distributed solution and multitenancy mode, IOC files can have the following types:

- **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.

- **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.

To view the list of supported OpenIOC indicators of compromise, you can download this file.

Users with the **Senior security officer** role can import, 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 computers with Kaspersky Endpoint Agent program installed.

Users with the **Security officer** and **Security auditor** roles can view the list of IOC files and information about the selected file, and export IOC files to their computer.

Viewing the table of IOC files

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 IOC files contains information about IOC files used for scanning on computers with the Kaspersky Endpoint Agent program installed; you can find the table in the **Custom 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 IOC file depending on the program operating mode and the server to which the IOC file was uploaded:

   - **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.
   - **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.

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**
   - **Disabled**

Viewing information about an IOC file

To view IOC file details:

1. In the window of the program web interface, select the **Custom 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** link opens the IOC file download window.

- **Autoscan**—The IOC file is used when automatically scanning Kaspersky Endpoint Agent hosts.
- **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 tenant and the names of servers associated with events scanned based on this IOC file (in 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 **Custom rules** section, **IOC** subsection.

   This opens the table of IOC files.
2. 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**—The IOC file is used when automatically scanning Kaspersky Endpoint Agent hosts:

   - **Enabled**
   - **Disabled**

   b. **Name**—Name of the IOC file.

   c. **Importance**—Importance level that will be assigned to an alert generated using this IOC file:

   - **Low**.
   - **Medium**.
   - **High**.

d. **Apply to**—Name of the tenant and names of the servers which you want to scan using this IOC file (in 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:

1. In the window of the program web interface, select the **Custom 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** 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 hosts

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 **Custom rules** section, **IOC** subsection.

   This opens the table of IOC files.
2. In the row 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**
   - **Disabled**

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 auditor** and **Security officer** roles cannot enable or disable automatic application of an 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 **Custom rules** section, **IOC** subsection.
2. This opens the IOC file table. 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 auditor** and **Security officer** roles 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 **Custom 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 events using an IOC file

To view events found using an IOC file:

1. In the window of the program web interface, select the **Custom 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 by required criteria:

1. In the window of the program web interface, select the **Custom 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**
  - **Disabled**

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 the IOC file filter for one or more filtering criteria:

1. In the window of the program web interface, select the **Custom 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 application web interface, select the **Settings** section, **Endpoint Agents** subsection, **IOC scanning schedule** section.
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 **Apply**.

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 auditor** and **Security officer** roles cannot configure the schedule for searching for indicators of compromise using IOC files on Kaspersky Endpoint Agent hosts.

Managing user-defined TAA (IOA) rules

Custom TAA (IOA) rules are created based on event databased search criteria. For example, if you want Kaspersky Anti Targeted Attack Platform to generate alerts for events when a program that you consider unsafe is started on Kaspersky Endpoint Agent computers, you can:

1. Generate a search query for the event database.
2. Create a custom TAA (IOA) rule based on event search conditions.

   When Central Node server receives events matching the created TAA (IOA) rule, Kaspersky Anti Targeted Attack Platform generates alerts.

You can also create a TAA (IOA) rule based on one or multiple event search criteria from the selected IOC file. To do so:

1. Upload an IOC file containing indicators of compromise corresponding to the malware to Kaspersky Anti Targeted Attack Platform.
2. Find events corresponding to the criteria of the selected IOC file.
3. Create a TAA (IOA) rule based on one or more event search criteria from the selected IOC file.

In distributed solution and multitenancy mode, TAA (IOA) rules can have one of the following types:

- **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 tenant which the user is managing in the program web interface.
- **Local**—Created on the SCN server. These rules are used to scan events on this SCN server. Scanned events belong to the tenant which the user is managing in the program web interface.

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 You can view recommendations in alert information
Correspondence to technique in MITRE ATT&CK database	No	Yes You can view the description of the technique according to the MITRE database in alert information
Display in the TAA (IOA) rule table	Yes	No
Ability to disable database lookup for this rule	Disable rule	Add rule to TAA exclusions
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

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 **Security officer** or **Security auditor** 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.

Viewing the TAA (IOA) rule table

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 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 **Custom 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 operating mode of the program and the role of the server which generated the rule:

   - **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 tenant which the user is managing in the program web interface.
   - **Local**—Created on the SCN server. These rules are used to scan events on this SCN server. Scanned events belong to the tenant which the user is managing in the program web interface.

3. **Confidence** is the 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.
   - **Disabled** – not displayed in the alert table.

7. **State** – usage status of the rule in event scans:

   - **Enabled** – the rule is being used.
   - **Disabled** – the rule is not being used.

Creating a TAA (IOA) rule based on event search conditions

To create a TAA (IOA) rule 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 **Save as TAA (IOA) rule**.

   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 **Custom 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 TAA (IOA) rule that you have created earlier will be unable to mark events by these fields.

Users with the **Security auditor** and **Security officer** roles cannot create TAA (IOA) rules based on event search conditions.

Importing a 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 that you test custom TAA (IOA) rules in a test environment before you import them. Custom TAA (IOA) rules may cause performance issues, in which case 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 **Custom 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. Set the **State** toggle switch to **Enabled** if you want to enable the rule for scanning the event 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.

Viewing custom TAA (IOA) rule details

To display information about the TAA (IOA) rule:

1. In the window of the program web interface, select the **Custom 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:

- Click the **Alerts** link to display the alert table in a new browser tab. The alerts are filtered by the Targeted Attack Analyzer technology and the name of the TAA (IOA) rule that you are working on.
- Click the **Find events** link to display the events table in a new browser tab. The table is filtered by rule name.
- Click the **Run query** link to display the events 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.
- Click the **IOA ID** link to display 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** is the 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 tenant which the user is managing in the program web interface.
  - **Local**—Created on the SCN server. These rules are used to scan events on this SCN server. Scanned events belong to the tenant which the user is managing in the program web interface.
- **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 **Custom 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) rules by required criteria:

1. In the window of the program web interface, select the **Custom 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 tenant which the user is managing in the program web interface.
     - **Local**—rules created on an SCN server. These rules are used to scan events on this SCN server. Scanned events belong to the tenant which the user is managing in the program web interface.

- **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
- **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**
  - **Disabled**

- **By rule state**

  a. Click **State** to expand the filter settings list.

  b. Select one of the following options:

  - **All**
  - **Enabled**
  - **Disabled**

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 **Custom rules** section, **TAA** subsection.
   This opens the TAA (IOA) rule table.
2. Click to the right of that column heading of the rule table for which you want to clear filtering criteria.

   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.

Enabling and disabling TAA (IOA) rules

Users with the **Senior security officer** role can enable or disable one or several rules, as well as all rules at once.

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 **Custom 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 **Custom 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 row 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.

In distributed solution and multitenancy mode, you can manage only global TAA (IOA) rules on the PCN server. You can manage local TAA (IOA) rules on SCN servers of tenants to which you have access.

Users with the **Security auditor** and **Security officer** roles cannot enable or disable TAA (IOA) rules.

Modifying a TAA (IOA) rule

Users with the **Senior security officer** role can modify custom TAA (IOA) rules. Rules created by Kaspersky cannot be edited.

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 edit a TAA (IOA) rule:

1. In the window of the program web interface, select the **Custom 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.

Users with the **Security auditor** and **Security officer** roles cannot modify TAA (IOA) rules based on event search conditions.

Deleting TAA (IOA) rules

Users with the **Senior security officer** role can delete one or more TAA (IOA) rules, or all rules at the same time.

In distributed solution and multitenancy 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 custom TAA (IOA) rule:

1. In the window of the program web interface, select the **Custom 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 custom TAA (IOA) rules:

1. In the window of the program web interface, select the **Custom 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 row 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.

Users with the **Security auditor** and **Security officer** roles cannot modify TAA (IOA) rules based on event search conditions.

Managing user-defined IDS rules

In distributed solution and multitenancy mode, custom IDS rules can have one of the following types:

- **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 tenant which the user is managing in the program web interface.
- **Local**—Created on the SCN server. These rules are used to scan events on this SCN server. Scanned events belong to the tenant which the user is managing in the program web interface.

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 auditor** 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.

Users with the **Security officer** role cannot gain access to user-defined IDS rules.

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 that you 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 program may create too many IDS alerts.
- If the program cannot record 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 program.
- Even formally correct user-defined rules may impact performance or cause faulty operation of the program.

IDs and attributes of custom rules may be modified when they are uploaded. Reject and Drop actions are changed to Alert. Rules with the Pass action are deleted

To import a custom IDS rule:

1. In the window of the program web interface, select the **Custom 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 **Custom 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 an IDS rule when scanning events:

1. In the window of the program web interface, select the **Custom rules** section, **IDS** subsection.
2. This opens the user-defined IDS rule window.

3. Move the **State** switch to one of the following positions:

   - **Enabled**
   - **Disabled**

   The use of the IDS rule when scanning events is enabled or disabled.

Users with the **Security auditor** role cannot enable or disable IDS rules.

Users with the **Security officer** role cannot gain access to user-defined IDS rules.

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 **Custom 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 necessary, use the **State** switch to enable this IDS rule.

   The importance of alerts generated using this IDS rule is configured.

Users with the **Security auditor** role cannot configure IDS rules.

Users with the **Security officer** role cannot gain access to user-defined IDS rules.

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 that you 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 they are uploaded. Reject and Drop actions are changed to Alert. Rules with the Pass action are deleted

To replace a custom IDS rule:

1. In the window of the program web interface, select the **Custom 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.

Users with the **Security auditor** role cannot replace user-defined IDS rules.

Users with the **Security officer** role cannot gain access to user-defined IDS rules.

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 custom IDS rule file to the computer:

1. In the window of the program web interface, select the **Custom 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, users with the **Senior security officer** role can delete only a user-defined IDS rule that was 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 custom IDS rule:

1. In the window of the program web interface, select the **Custom 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.

Users with the **Security auditor** role cannot delete user-defined IDS rules.

Users with the **Security officer** role cannot gain access to user-defined IDS rules.

Managing user-defined YARA rules

You can use YARA rules as YARA module databases to scan files and objects received at the Central Node and to scan hosts that have Kaspersky Endpoint Agent for Windows installed.

In distributed solution and multitenancy mode, custom YARA rules can have one of the following types:

- **Global**—Created on the PCN server. These rules are used to scan files and objects received at the PCN server and all SCN servers connected to that PCN server. Scanned files and objects belong to the tenant which the user is managing in the program web interface.
- **Local**—Created on the SCN server. These rules are used to scan files and objects received at the SCN server. Scanned files and objects belong to the tenant which the user is managing in the program web interface.

When managing the program web interface, users with the **Senior security officer** role can import a YARA rule file into Kaspersky Anti Targeted Attack Platform using the program web interface.

Users with the **Security auditor** and **Security officer** roles can only view YARA rules.

Viewing the YARA rule table

The table of user-defined YARA rules contains information about YARA rules that are used to scan events and create alerts; the table is displayed in the **Custom rules** section, **YARA** subsection of the program web interface window.

The table contains the following information:

- **Created** is the rule creation time.
- —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.

  By default, alerts generated by uploaded YARA rules are assigned a high level of importance.
- **Type** is the type of the rule depending on the operating mode of the program and the role of the server which generated the rule:
  - **Global**—Created on the PCN server. These rules are used to scan files and objects received at the PCN server and all SCN servers connected to that PCN server. Scanned files and objects belong to the tenant which the user is managing in the program web interface.
  - **Local**—Created on the SCN server. These rules are used to scan files and objects received at the SCN server. Scanned files and objects belong to the tenant which the user is managing in the program web interface.
- **Name** – name of the rule.
- **File name** is the name of the file from which the rule was imported.
- **Created by** is the name of the user whose account was used to import the rule.
- **Servers** – name of the server with the Central Node component on which the rule is applied.
- **Traffic scan** is the usage status of the rule when stream scanning files and objects arriving at the Central Node:
  - **Enabled** – the rule is being used.
  - **Disabled** – the rule is not being used.

Importing YARA rules

To import YARA rules:

1. In the window of the program web interface, select the **Custom 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 and opens the **Import YARA rules** window.

   The maximum allowed size of an uploaded file is 20 MB.

A report is displayed in the lower part of the window. The report contains the following information:

- The number of rules that can be successfully imported.
- The number of rules that will not be imported (if any).

  For each rule that cannot be imported, its name is listed.

4. Select the **Traffic scan** check box if you want to use imported rules for streaming scans of objects and data received at the Central Node.
5. If necessary, enter any additional information in the **Description** field.

   The **Importance** field cannot be edited. By default, alerts generated by uploaded YARA rules are assigned a high level of importance.

6. Under **Apply to**, select check boxes corresponding to servers on which you want to apply the rules.

   This field is displayed only when you are using the distributed solution and multitenancy mode.

7. Click **Save**.

Imported rules are displayed in the table of YARA rules.

Configuring YARA rule table display

You can show or hide columns and change the order of columns in the table.

To configure the table display:

1. In the window of the application web interface, select the **Custom rules** section, **YARA** subsection.

   This opens the YARA rule table.

2. In the heading part of the table, click .

   This opens the **Customize table** window.

3. If you want to show a column in the table, select the check box next to the name of the parameter that you want displayed in the table.

   If you want to hide a parameter in the table, clear the check box.

   At least one check box must be selected.

4. If you want to change the order of columns in the table, move the mouse cursor to the row with the relevant parameter, click and move the row to its new place.
5. If you want to restore default table display settings, click **Default**.
6. Click **Apply**.

The table display is configured.

Viewing YARA rule details

To view YARA rule details:

1. In the window of the program web interface, select the **Custom rules** section, **YARA** subsection.

   This opens the YARA 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:

- Click the **Alerts** link to display the alert table in a new browser tab. The alerts are filtered by the Targeted Attack Analyzer technology and the name of the TAA (IOA) rule that you are working on.
- The **Start YARA scan** link opens the task creation window.
- The **Download** link lets you download a file with YARA rules.
- **Rule name** is the name of the rule specified in the file.
- **Traffic scan** is the usage status of the rule when stream scanning files and objects arriving at the Central Node:
- **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 files and objects received at the PCN server and all SCN servers connected to that PCN server. Scanned files and objects belong to the tenant which the user is managing in the program web interface.
  - **Local**—Created on the SCN server. These rules are used to scan files and objects received at the SCN server. Scanned files and objects belong to the tenant which the user is managing in the program web interface.
- **Importance**—Importance level that is assigned to an alert generated using this rule.

  By default, alerts generated by uploaded YARA rules are assigned a high level of importance.
- **Description** is any additional information about the rule that you specified.
- **Apply to**—Name of servers with the Central Node component on which the rule is applied.

Filtering and searching YARA rules

To filter or search for YARA rules by required criteria:

1. In the window of the application web interface, select the **Custom rules** section, **YARA** subsection.

   This opens the YARA rule table.

2. Depending on the filtering criterion, do the following:

- **By creation time**

  a. Click the **Created** link to open the filter settings window.

  b. Select one of the following options:

  - **Any time** if you want the table to display rules created at any time.
  - **Last hour** if you want the application to display the rules that were created during the last hour in the table.
  - **Last day** if you want the application to display the rules that were created during the last day in the table.
  - **Custom range** if you want the application to display the rules that were created during the period you specify in the table.

  c. If you selected **Custom range**, select the start and end dates for the period and click **Apply**.

- **By rule name**

  a. Click the **Rule name** link to open the filtering menu.

  b. In the drop-down list, select one of the following filtering operators:

  - **Contains**
  - **Does not contain**

  c. In the text box, type the name of the rule or a sequence of characters from the name of the rule.

  d. Click **Apply**.

- **By file name**

  a. Click the **File name** link to open the filtering menu.

  b. In the drop-down list, select one of the following filtering operators:

  - **Contains**
  - **Does not contain**

  c. In the entry field, type the name of the file or a sequence of characters from the name of the file.

  d. Click **Apply**.

- **By the name of the user who uploaded the rules file**

  a. Click the **Created by** link to open the filtering menu.

  b. In the drop-down list, select one of the following filtering operators:

  - **Contains**
  - **Does not contain**

  c. In the text box, type the user name or a sequence of characters from the user name.

  d. Click **Apply**.

- **By rule state**

  a. Click the **Traffic scanning** link to expand the filter settings list.

  b. Select one of the following options:

  - **All**
  - **Enabled**
  - **Disabled**

The table displays only rules that match the specified criteria.

You can use multiple filters at the same time.

Clearing a YARA rule filter

To clear the YARA rule filter for one or more filtering criteria:

1. In the window of the application web interface, select the **Custom rules** section, **YARA** subsection.
   This opens the YARA rule table.
2. Click to the right of that column heading of the rule table for which you want to clear filtering criteria.
   If you want to clear multiple filter conditions, take steps to clear each filter condition individually.

The selected filters are cleared.

The table displays only rules that match the specified criteria.

Enabling and disabling YARA rules

Users with the **Senior security officer** role can enable or disable one or several rules, as well as all rules at once.

When working in distributed solution and multitenancy mode, you can enable or disable only those YARA rules that were created on the current server. It means that in the web interface of the PCN, you can enable or disable only the rules that were created on the PCN server. In the web interface of an SCN, you can enable or disable only the rules that were created on the SCN server.

If YARA rules with identical names are enabled on the PCN and SCN servers, the PCN rule takes precedence over the SCN rule when scanning files and objects.

To enable or disable a YARA rule for stream scanning files and objects arriving at the Central Node:

1. In the window of the program web interface, select the **Custom rules** section, **YARA** subsection.
   This opens the YARA rule table.
2. In the row with the relevant rule, select or clear the check box in the **Traffic scan** column.

The rule is enabled or disabled for stream scanning files and objects arriving at the Central Node.

To enable or disable all or multiple YARA rules for stream scanning files and objects arriving at the Central Node:

1. In the window of the program web interface, select the **Custom rules** section, **YARA** subsection.
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 row 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.

Selected rules are enabled or disabled for stream scanning files and objects arriving at the Central Node.

Deleting YARA rules

To delete a YARA rule:

1. In the window of the program web interface, select the **Custom rules** section, **YARA** subsection.
   This opens the YARA rule table.
2. Select the rule that you want to delete.
   This opens a window containing information about the rule.

3. Click **Delete**.
4. This opens the action confirmation window; in that window, click **Yes**.

The rule is deleted.

To delete all or multiple YARA rules:

1. In the window of the program web interface, select the **Custom rules** section, **YARA** subsection.

   This opens the YARA 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 row containing the headers of columns.

   A control panel appears in the lower part of the window.
3. Click **Delete**.
4. This opens the action confirmation window; in that window, click **Yes**.

The selected rules will be deleted.

Users with the **Security auditor** and **Security officer** roles cannot delete YARA rules.

Managing objects in Storage and Quarantine

Storage is used for storing files that must be sent for scanning as well as files obtained as a result of running tasks: **Get file**, **Restore file from quarantine**, **Get forensics**, **Get NTFS metafiles**, **Get registry key**, **Get process memory dump**.

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, Storage is located on PCN and SCN servers. The web interface of the PCN server displays information about Storage of all connected SCNs for those tenants to which the user has access.

Users with the **Senior security officer** role can place copies of objects into Storage using tasks or by uploading the object to Storage using the Kaspersky Anti Targeted Attack Platform web interface on the PCN or SCN server that is used for managing tenants to which the user has 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 tenants to which the user has 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:
     - The **Get file** task was run.
     - 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 placed in Storage in one of the following ways:
     - The **Get forensics** task was run.
     - The **Get process memory dump** task was run.

- The **Get registry key** task was run.
- The **Get NTFS metafiles** task was run.

- – 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. **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. **Record time**—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:

- **Add to filter**.
- **Exclude from filter**.
- **Download**.
- **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:

- **Add to filter**.
- **Exclude from filter**.
- Find events.
- Find alerts.
- **Copy value to clipboard**.

Viewing information about an object manually placed in Storage using the web interface

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.
3. 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 TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

Click **Create 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 TIP**.
- **Find events**.
- **Find alerts**.
- **Create 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 TIP**.
- **Find on virustotal.com**.
- **Find events**.
- **Find alerts**.
- **Create prevention rule**.
- **Copy value to clipboard**.

Viewing information about an object placed in Storage by a get file task

*To view information about an object placed in Storage by a **Get file** or **Get file from quarantine** task:*

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table.

3. 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.
- **Record time**—Time when the object was placed in Storage.
- **Tenant** —Name of the tenant 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 TIP** button allows to find a file on the Kaspersky Threat Intelligence Portal.

Click **Create 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 TIP**.
- **Find events**.

- Find alerts.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find events.
- Find alerts.
- Create prevention rule.
- **Copy value to clipboard**.

Viewing information about an object placed in Storage by a get data task

*To view information about an object placed in Storage by **Get forensics**, **Get process memory dump**, **Get registry key**, **Get NTFS metafiles** tasks:*

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:

- **Object**—File name or path.
- **Size**—Size of the file.
- **MD5**—MD5 hash of a file.
- **SHA256**—SHA256 hash of a file.
- **Record time**—Time when the object was placed in Storage.
- **Host**—Name of the host from which the object was received.

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 TIP.
- Find events.
- Find alerts.
- Create 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 TIP.
- **Find on virustotal.com**.
- Find events.
- Find alerts.
- Create 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 line with the name of the object that you want to download, click .

   The object will be saved to your local computer in the browser's downloads folder. The file is downloaded as a ZIP archive protected with the password "infected".

Uploading objects to 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 the **Upload** button.
   This opens the file selection window.
3. Select the object that you want to upload to Storage.
4. If you want to upload a file with the .Lnk extension to Storage:
   a. In the **File name** field, enter *.Lnk and press **Enter**.
   b. Select the object.
5. Click **Open**.

The object will be uploaded to Storage and will be displayed in the table of objects.

Users with the **Security auditor** role cannot upload objects to Storage.

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 for scanning:

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.

Users with the **Security auditor** role cannot scan objects 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 from 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.

Users with the **Security auditor** role cannot delete objects in 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:
   - **Uploaded by a Get file task** if you want the table to display objects that were placed in Storage by **Get file** and **Restore file from quarantine** tasks.
   - **Uploaded through the web interface** if you want the table to display objects uploaded by the user using the Kaspersky Anti Targeted Attack Platform web interface.
   - **Uploaded by a get data task** if you want the table to display objects placed in Storage by **Get forensics**, **Get NTFS metafiles**, **Get registry key**, **Get process memory dump** tasks.
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 by 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 by 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 by the name of 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 by 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 **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 by the time when they were placed in Storage:

1. In the program web interface window, select the **Storage** section, **Files** subsection.
2. This opens the object table. Click the **Record time** 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 the Storage objects filter for one or more filtering criteria:

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 program 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. **Source**—IP address or host name of the computers with the Kaspersky Endpoint Agent program where the object is quarantined.
3. **Record time**—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:

- **Add to filter**.
- **Exclude from filter**.
- **Download**.
- **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:

- **Add to filter**.
- **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 program 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.
- **Tenant** —Name of the tenant to which the Central Node, PCN, or SCN server belongs.
- **Host**—Computer name 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 a computer with the Kaspersky Endpoint Agent program:

1. In the program web interface window, select the **Storage** section, **Quarantine** subsection.

   This opens the object table.

2. 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 and the **Restore file from quarantine** task.

4. In the **Description** field, enter the task description.

5. Click **Add**.

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.

Users with the **Security auditor** role cannot restore objects from Quarantine.

Obtaining a copy of a quarantined object on a Kaspersky Anti Targeted Attack Platform server

The object that you want to download a copy of must not exceed 100 MB. If the object exceeds 100 MB, the task finishes with an error.

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 program web interface window, select the **Storage** section, **Quarantine** subsection.

   This opens the object table.

2. 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.

   This creates a task for getting a copy of an object that was quarantined on a Kaspersky Endpoint Agent computer. If the task completes successfully, the copy of the object is uploaded to the Kaspersky Anti Targeted Attack Platform server. The object is displayed in the **Storage** section, **Files** subsection of the program web interface in the table of objects placed in Storage.

   Information about the created task is displayed in the **Tasks** section of the web interface.

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.

Users with the **Security auditor** role cannot get copies of objects from Quarantine.

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 program 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.

Users with the **Security auditor** role cannot delete information about a quarantined object from the table.

Filtering information about quarantined objects by object type

To filter quarantined object details by object type:

1. In the application web interface window, select the **Storage** section, **Quarantine** subsection.
   This opens the object table.
2. Click the **Type** link to open the object filtering menu.
3. Select one or more check boxes:
   - **File** if you want the table to display metadata of quarantined objects.
   - **Process memory dump** if you want the table to display metadata of quarantined dumps.
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 information about quarantined objects by object description

To filter quarantined object details by object description:

1. In the program 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 quarantined object details by the name of the host where they were quarantined:

1. In the program web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. Click the **Source** link to open the object filtering menu.
3. In the drop-down list, select one of the following object filtering operators:
   - **Contains**
   - **Does not contain**
4. In the entry field, specify one or several characters of the 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 quarantined object details by the time when they were quarantined:

1. In the program web interface window, select the **Storage** section, **Quarantine** subsection.
2. This opens the object table. Click the **Record time** 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 clear the filter for one or more filtering criteria:

1. In the program 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 managing 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.

Users with the **Security auditor** role can view reports and report templates and create reports from 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 tenant and servers of that tenant.

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.

Users with the **Security officer** role do not have access to reports.

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.

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.

A new report template is created for each data sample.

To create a template:

1. In the program web interface window, select the **Reports** section, **Templates** tab.

   This opens the table of templates.

2. Click **Add**.

   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 **Data source** 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**, 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.

Users with the **Security auditor** and **Security officer** roles cannot create report templates.

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 **Add**.

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 tenants and servers whose data you want to include 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.

Users with the **Security officer** role cannot create report templates.

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 the report 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**.

     - **Data source**.

     - **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 the template and click **Save as**.

     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.

Users with the **Security auditor** and **Security officer** roles cannot edit templates.

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 by creation time:

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 the template filter for one or more filtering criteria:

1. In the program web interface window, select the **Reports** section, **Templates** tab.
2. This opens the table of templates. Click to the right of the header of the column of the template table 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 delete 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.

Users with the **Security auditor** and **Security officer** roles cannot delete templates.

Filtering reports by creation time

To filter reports by 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 by 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 by the name of the user that created 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 the report filter for one or more filtering criteria:

1. In the window of the program web interface, select the **Reports** section, **Generated Reports** subsection.

   This opens the table of reports.

2. Click to the right of the header of the column of the reports table 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.

Users with the **Security auditor** and **Security officer** roles cannot delete reports.

Managing rules for assigning the VIP status to alerts

Users with the **Senior security officer** role can create, delete, modify, import and export a list of rules for assigning the VIP status to alerts.

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.

Users with the **Security auditor** role can view, import and export a list of rules for assigning the VIP status to alerts.

Users with the **Security officer** role cannot view the list of rules for assigning VIP status to alerts.

Viewing the table of VIP status assignment rules

The table of rules for assigning the VIP status is located in the **Settings** section, **VIP status** subsection of the web interface of the application.

The table contains the following information:

- **Criterion**—Criterion for adding an entry to the list of rules.
- **Value**—Value of the criterion.
- **Description**—Additional information specified when creating the rule.

Creating a VIP status assignment rule

To add a rule for assigning the VIP status to alerts:

1. In the main window of the program web interface, select the **Settings** tab, **VIP status** section.
2. In the upper-right corner of the program web interface window, click **Add**.

   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 **Add**.

The rule is added. The VIP status will be assigned to new alerts associated with the added IP address, host name, or email address.

Users with the **Security auditor** role cannot create VIP status assignment rules.

Users with the **Security officer** role cannot view the list of rules for assigning VIP status to alerts.

Deleting a VIP status assignment rule

To delete a rule for assigning the VIP status to alerts:

1. In the main window of the program web interface, select the **Settings** tab, **VIP status** section.

2. Select the check box to the left of each rule that you want to remove from the list.

3. If you want to delete all rules, select the check box above the list.

4. In the upper-right corner of the program web interface window, click the **Delete** button.

   The action confirmation window is displayed.

5. Click **Yes**.

The selected rules will be deleted.

Users with the **Security auditor** role cannot delete VIP status assignment rules.

Users with the **Security officer** role cannot view the list of rules for assigning VIP status to alerts.

Modifying a VIP status assignment rule

To modify a rule for assigning the VIP status to alerts:

1. In the main window of the program web interface, select the **Settings** tab, **VIP status** section.

2. Select the rule that you want to modify.

   This opens the rule editing window.

3. Make the necessary changes to the **Criteria**, **Value** and **Description** fields.

4. Click **Save**.

The rule is modified.

Users with the **Security auditor** role cannot modify VIP status assignment rules.

Users with the **Security officer** role cannot view the list of rules for assigning VIP status to alerts.

Importing a list of VIP status assignment rules

To import a list of rules for assigning VIP status to alerts:

1. In the main window of the program web interface, select the **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 the list of rules for assigning VIP status to alerts:

1. In the main window of the program web interface, select the **Settings** tab, **VIP status** section.

2. In the upper-right corner of the program web interface window, click the **Export** button.

The list of VIP status assignment rules is exported to a JSON file.

Filtering and searching by type of VIP status assignment rule

To filter or search for VIP status assignment rules by rule type:

1. In the main window of the program web interface, select the **Settings** tab, **VIP status** section.
2. Click the **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 **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 **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 the VIP status assignment rule filter for one or more filtering criteria:

1. In the main window of the program web interface, select the **Settings** tab, **VIP status** section.
2. Click  to 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 list of scan exclusions

Users with the **Senior security officer** role can create, import and export the *list of scan exclusions*, that is, the list of data that Kaspersky Anti Targeted Attack Platform treats as safe and does not display in the alerts table. You can create scan exclusion rules for the following data:

- **MD5**
- **Format**
- **URL mask**
- **Email recipient**
- **Email sender**
- **Source IP or subnet**
- **Destination IP or subnet**
- **User Agent**

Users with the **Security auditor** and **Security officer** roles can view the list of scan exclusion rules, as well as export it.

Viewing the table of data excluded from the scan

To view the table with data excluded from the scan:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.

   This opens the table with a list of data that Kaspersky Anti Targeted Attack Platform will treat as safe and will not create alerts for. You can filter the rules by clicking links in column headers.

The table contains the following information:

- **Criteria**—Criterion for adding an entry to the list of allowed objects.
- **Value**—Value of the criterion.

Adding a scan exclusion rule

To add to scan exclusions:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.
3. In the upper-right corner of the program web interface window, click **Add**.

   This opens the **New rule** window.
4. In the **Criteria** drop-down list, select one of the following criteria for adding a rule to the list of scan exclusions:

   - **MD5**
   - **Format**
   - **URL mask**
   - **Email recipient**
   - **Email sender**
   - **Source IP or subnet**
   - **Destination IP 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 IP or subnet**, **Destination IP or subnet**, or **User Agent**, in the **Value** field, enter the value of the relevant criterion that you want to add to the list of scan exclusions:

   - 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 list of scan exclusions, use the `\` character when entering the URL to escape 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 list of scan exclusions 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 IP or subnet** or **Destination IP or subnet**, enter the address or subnet (for example, 255.255.255.0) in the **Value** field.

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 **Add**.

The rule is added to the scan exclusion list.

Users with the **Security auditor** and **Security officer** roles cannot add a scan exclusion rule.

Deleting a scan exclusion rule

To remove one or multiple rules from scan exclusions:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.
3. Select the check box to the left of each rule that you want to remove from the list of scan exclusions.
   If you want to delete all rules, 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 rules are removed from the list of scan exclusions.

Users with the **Security auditor** and **Security officer** roles cannot remove entries from the list of scan exclusions.

Editing a rule added to scan exclusions

To edit a rule in the scan exclusion list:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.
3. Select the rule that you want to modify.

   This opens the **Edit rule** window.
4. Make the necessary changes to the **Criteria** and **Value** fields.
5. Click **Save**.

The rule is modified.

Users with the **Security auditor** and **Security officer** roles cannot edit rules in the list of scan exclusions.

Exporting the list of data excluded from the scan

To export the scan exclusion list:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.
3. In the upper-right corner of the program web interface window, click the **Export** button.

The JSON file containing the exported list of scan exclusions is saved in the browser's downloads folder on your computer.

Filtering rules in the scan exclusion list by criterion

To filter scan exclusion list entries by rule type:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** 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 the rules:

   - **MD5**
   - **Format**
   - **URL mask**
   - **Email recipient**
   - **Email sender**
   - **Source IP or subnet**
   - **Destination IP or subnet**
   - **User Agent**

5. Click **Apply**.

   The filter configuration window closes.

   The list of scan exclusions displays only those rules that match your criteria.

You can use multiple filters at the same time.

Searching rules in the scan exclusion list by value

To search rules in the scan exclusion list by value:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.
3. Click the **Value** link to open the filter configuration window.
4. Enter value characters.
5. Click **Apply**.

   The list of scan exclusions displays only those rules that match your criteria.

You can use multiple filters at the same time.

Resetting the rule filter in the scan exclusion list

To clear an exclusion list record filter by one or more filtering criteria:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **Scan exclusions** tab.
3. Click to the right of the header of the column in the table of scan exclusion list entries 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 list of scan exclusions displays only those rules that match your criteria.

Managing IDS exclusions

Users with the **Senior security officer** role can add Kaspersky IDS rules that have resulted in medium or high importance alerts to scan exclusions. 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 when scanning, you can disable this rule or delete it.

Users with the **Security auditor** role can view the list of IDS rules added to exclusions, and view the properties of a selected rule.

Users with the **Security officer** role cannot view the list of IDS rules added to exclusions.

Viewing the table of Intrusion Detection rules added to exclusions

To view the table of Intrusion Detection rules added to exclusions:

1. In the main window of the application web interface, select the **Settings** section, **Exclusions** subsection.
2. Go to the **IDS** tab.

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 Intrusion Detection rule was added to exclusions.
- **Rule name**—Name of the Intrusion Detection rule.
- **Rule ID**—ID of the Intrusion Detection rule (SID or signature ID) in Suricata format.
- **Description**—Description of the Intrusion Detection rule.
- **Created by**—Name of the user whose account was used to add the Intrusion Detection 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 exclusions**.

   This opens the **Add IDS rule to exclusions** window.

10. In the **Description** field, enter a description for the IDS rule.

11. Click **Add**.

    The IDS rule is added to exclusions and is displayed in the exclusion list in the **Settings** section, **Exclusions** subsection on the **IDS exclusions** in the program web interface. This rule is no longer used for creating alerts.

Users with the **Security auditor** role cannot modify entries in the list of allowed objects.

Users with the **Security officer** role do not have access to the list of IDS rules added to exclusions.

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 exclusion**.

   This opens the **Edit IDS exclusion** 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.

Users with the **Security auditor** role cannot edit IDS rule descriptions.

Users with the **Security officer** role do not have access to the list of IDS rules added to exclusions.

Removing an 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 **Settings** → **Exclusions** section and go to the **IDS exclusions** 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 **Settings** → **Exclusions** section and go to the **IDS exclusions** 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 row 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.

Users with the **Security auditor** role cannot remove IDS rules from exclusions.

Users with the **Security officer** role do not have access to the IDS exclusion list.

Managing TAA exclusions

TAA (IOA) rules created by Kaspersky experts contain indicators of suspicious behavior of an object in the corporate IT infrastructure. Kaspersky Anti Targeted Attack Platform scans the events database of the program and creates alerts for events that match behaviors described by TAA (IOA) rules. If you do not want the program to create alerts for events generated as part of host activity that is normal for your organization, you can add a TAA (IOA) rule to exclusions.

TAA (IOA) rule modes added to exclusions can work in the following modes:

- The rule is always excluded.

  In this case, Kaspersky Anti Targeted Attack Platform does not mark events as matching the TAA (IOA) rule and does not create alerts based on that rule.

- The rule is supplemented by a condition.

  In this case, the TAA (IOA) rule is supplemented by conditions in the form of a search query. Kaspersky Anti Targeted Attack Platform does not mark events that match specified conditions as matching the TAA (IOA) rules. For events that match the TAA (IOA) rule, but do not satisfy the conditions of the applied exclusion, the program marks the events and creates alerts.

If you are using the distributed solution and multitenancy mode, TAA exclusions can have the following types:

- **Local**—Created on the SCN server. These exclusions apply only to hosts that are connected to this SCN server. Exclusions belong to the tenant which the user is managing in the program web interface.

- **Global**—Created on the PCN server. Exclusions apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Exclusions belong to the tenant which the user is managing in the program web interface.

Users with the **Senior security officer** role can create, edit, and delete exclusions for tenants to whose data they have access.

Users with the **Security auditor** and **Security officer** roles can only view the list of TAA exclusions and the properties of a selected exclusion.

For each TAA (IOA) rule, you can create only one local or global exclusion.

If one TAA (IOA) rule has exclusions created both on an SCN server and the PCN server, Kaspersky Anti Targeted Attack Platform processes events in accordance with exclusion settings on the PCN server.

Viewing the table of TAA (IOA) rules added to exclusions

To view the table of TAA (IOA) rules added to exclusions:

1. In the main window of the program web interface, select the **Settings** section, **Exclusions** subsection.
2. Click the **TAA exclusions** tab.

   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:

- —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**.
- **Type** is the type of the rule depending on the role of the server which generated it:
  - **Local**—Created on the SCN server. These exclusions apply only to hosts that are connected to this SCN server. Exclusions belong to the tenant which the user is managing in the program web interface.
  - **Global**—Created on the PCN server. Exclusions apply to hosts that are connected to this PCN server and to all SCN servers that are connected to this PCN server. Exclusions belong to the tenant which the user is managing in the program web interface.
- **Confidence** is the level of confidence depending on the likelihood of false alarms caused by the rule:
  - **High**.
  - **Medium**.
  - **Low**.

  The higher the confidence level, the lower the likelihood of false alarms.

- **Exclude rule** is the operating mode of the rule that is added to exclusions.
  - **Always** means the rule is always excluded. In this case, Kaspersky Anti Targeted Attack Platform does not mark events as matching the TAA (IOA) rule and does not create alerts based on that rule.
  - **Based on conditions** means the rule is excluded if a condition is added. In this case, the TAA (IOA) rule is supplemented by conditions in the form of a search query. Kaspersky Anti Targeted Attack Platform does not mark events that match specified conditions as matching the TAA (IOA) rules. For events that match the TAA (IOA) rule, but do not satisfy the conditions of the applied exclusion, the program marks the events and creates alerts.
- **Name** is the name of the rule.

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 custom 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 exclusions** setting name, click **Add to exclusions**.
   This opens a window that allows you to add the TAA (IOA) rule to exclusions.
9. In the **Exclude rule** field, select the exclusion operating mode:
   - **Always** if you do not want the program to create alerts for events that match the selected TAA (IOA) rule.
   - **Based on conditions** if you do not want the program to create alerts only for events that match specified conditions. Alerts are created for events that match the TAA (IOA) rule with the configured exclusion conditions taken into account.

If you selected **Based on conditions**:

a. Click **Configure additional conditions** to open the event search form.

b. If you are using the distributed solution and multitenancy mode and want to enable the display of events for all tenants, turn on the **Search in all tenants** toggle switch.

c. Perform an event search in design mode.

A table is displayed of events that match the TAA (IOA) rule given the specified exclusion criteria.

If you are using the distributed solution and multitenancy mode, found events are grouped in tiers: Server – Tenant names – Server names.

d. Click the name of the server for which you want to view events.

The host table of the selected server is displayed. Event grouping levels are displayed above the table.

> If necessary, you can change event search conditions.

e. Click **Add exclusion**.

10. If you are using the distributed solution and multitenancy mode, in the **Apply to servers*** field, select check boxes for tenants and servers to which the rule must be applied.

11. Click **Add**.

The TAA (IOA) rule is added to exclusions and is displayed in the exclusion list in the **Settings** section, **Exclusions** subsection on the **TAA exclusions** 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 exclusions** setting name, click **Add to exclusions**.

This opens a window that allows you to add the TAA (IOA) rule to exclusions.

6. In the **Exclude rule** field, select the exclusion operating mode:

- **Always** if you do not want the program to create alerts for events that match the selected TAA (IOA) rule.
- **Based on conditions** if you do not want the program to create alerts only for events that match specified conditions. Alerts are created for events that match the TAA (IOA) rule with the configured exclusion conditions taken into account.

If you selected **Based on conditions**:

a. Click **Configure additional conditions** to open the event search form.

b. If you are using the distributed solution and multitenancy mode and want to enable the display of events for all tenants, turn on the **Search in all tenants** toggle switch.

c. Perform an event search in design mode.

A table is displayed of events that match the TAA (IOA) rule given the specified exclusion criteria.

If you are using the distributed solution and multitenancy mode, found events are grouped in tiers: Server – Tenant names – Server names.

d. Click the name of the server for which you want to view events.

The host table of the selected server is displayed. Event grouping levels are displayed above the table.

If necessary, you can change event search conditions.

e. Click **Add exclusion**.

7. Click **Add**.

The TAA (IOA) rule is added to exclusions and is displayed in the exclusion list in the **Settings** section, **Exclusions** subsection on the **TAA exclusions** tab in the program web interface. This rule is no longer applied when scanning events.

When creating a search query to be saved as an exclusion criterion, avoid using the following fields:

- IOAId.
- IOATag.
- IOATechnique.
- IOATactics.
- IOAImportance.
- IOAConfidence.

These fields are only displayed after Kaspersky Anti Targeted Attack Platform marks events as matching TAA (IOA) rules.

Users with the **Security auditor** and **Security officer** roles cannot add TAA (IOA) rules to exclusions.

Viewing a TAA (IOA) rule added to exclusions

To view a TAA (IOA) rule added to exclusions:

1. In the program web interface window, select the **Settings** section, **Exclusions** subsection and go to the **TAA exclusions** tab.

   The table of excluded TAA (IOA) rules is displayed.

2. 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 information about 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.
- **Exclude rule** is the operating mode of the rule that is added to exclusions.
  - **Always** means the rule is always excluded. In this case, Kaspersky Anti Targeted Attack Platform does not mark events as matching the TAA (IOA) rule and does not create alerts based on that rule.
  - **Based on conditions** means the rule is excluded if a condition is added. In this case, the TAA (IOA) rule is supplemented by conditions in the form of a search query. Kaspersky Anti Targeted Attack Platform does not mark events that match specified conditions as matching the TAA (IOA) rules. For events that match the TAA (IOA) rule, but do not satisfy the conditions of the applied exclusion, the program marks the events and creates alerts.
- **Configure additional conditions**: click this link to open the event search form with search conditions.

  The field is displayed if, when adding the TAA (IOA) rule to exclusions, you have selected the **Based on conditions** mode, and configured some search criteria.
- The search criteria are configured in the `<IOA ID> AND NOT <search criteria>` format.

  Search criteria are displayed if, when adding the TAA (IOA) rule to exclusions, you have selected the **Based on conditions** mode, and configured some search criteria.
- **Apply to servers*** are hosts to which the exclusion applies.

  This field is displayed in distributed solution and multitenancy mode.

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 **Settings** section, **Exclusions** subsection and go to the **TAA exclusions** tab.

   The table of excluded TAA (IOA) rules is displayed.

2. Select the rule that you want to remove from exclusions.

   This opens a window containing information about the rule.

3. Click **Delete**.

   This opens the action confirmation window.

4. 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 **Settings** section, **Exclusions** subsection and go to the **TAA exclusions** 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 row 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.

Users with the **Security auditor** and **Security officer** roles cannot remove TAA (IOA) rules from exclusions.

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 archive passwords:

1. In the window of the program web interface, select the **Settings** section, **Passwords for archives** subsection.
2. In the **Passwords for 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.

Users with the **Security auditor** role can view the list of passwords for archives, but cannot edit it.

Viewing server settings

Users with the **Security auditor** role can view Central Node server and PCN settings in distributed solution and multitenancy mode.

The server settings are located in the **Settings** section of the web interface window. In this section, you can view the following information:

- **Users**—List of user accounts of program web interface users.
- **General settings**—General settings of the server.
  - **Database update**—Database update.
  - **Monitoring**—Maximum allowed hard disk space usage for Central Node and Sensor servers.
  - **SNMP**—SNMP connection settings.
  - **Server management**—server management.

- **Certificates**—Status of server certificates and computers with Kaspersky Endpoint Agent program.
- **Date and time**—Server date and time settings.
- **Endpoint Agents**—Program functionality available when integrating with Kaspersky Endpoint Agent.
  - **IOC scanning schedule**—Settings for the IOC scan schedule.
  - **Send files to Sandbox automatically**—Automatically send files to be scanned by the Sandbox component.
  - **Activity indicators**—Activity indicators of Kaspersky Endpoint Agent.
- **KSN/KPSN and MDR**—Settings for participation in Kaspersky Security Network and Kaspersky Private Security Network.
- **KPSN reputation database**—Settings for using the KPSN reputation database.
- **SIEM system**—Settings for integration with a SIEM system.
- **Notifications**—Settings for sending notifications.
- **VIP status**—List of rules for assigning the VIP status to alerts.
- **Exclusions**—List of allowed objects and lists of exclusions from TAA and IDS rules.
- **Network settings**—Settings for the network interface parameters.
- **Passwords for archives**—List of passwords for archives.
- **License**—State of the license key.
- **Activity log**—Settings for the activity log.

Viewing the table of servers with the Sandbox component

Users with the **Senior security officer** and **Security officer** roles cannot view the table of servers with the Sandbox component.

Users with the **Security auditor** role can view the table of servers with the Sandbox component.

The table of servers with the Sandbox component is located on the **Sandbox servers** tab of the program web interface window.

The table contains the following information:

- **IP and name**—IP address or fully qualified domain name of the server with the Sandbox component.
- **Certificate fingerprint**—Certificate fingerprint of the server with the Sandbox component.

- **Authorization**—Status of the request to connect to the Sandbox component.
- **Status**—Status of the connection to the Sandbox component.

Viewing the table of servers with the Sensor component

Users with the **Security auditor** role can view the table of servers with the Sensor component.

- 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.

Users with the **Senior security officer** and **Security officer** roles cannot view the table of servers with the Sensor component.

Viewing the table of external systems

Users with the **Security auditor** role can view the table of external systems.

The table of external systems is in the **External systems** section of the application web interface window.

The **Certificate fingerprint** field displays the fingerprint of the TLS certificate of the Central Node server.

The **Server list** 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 Central Node server.

  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.

Users with the **Senior security officer** and **Security officer** roles cannot view the table of external systems.

Sending notifications

Users with the **Administrator**, **Senior security officer**, or **Security officer** role can configure forwarding of notifications to one or multiple email addresses.

You can create notifications about alerts and system health.

Users with the **Security auditor** role can view the list of rules for sending notifications, the properties of a selected rule, and the mail server connection settings, but cannot edit them.

For notifications to be sent to an email address correctly, you must first configure the connection to the mail server. The connection must be configured by the **Administrator**.

Viewing the table of rules for sending notifications

Rules for sending notifications are displayed in the **Settings** section, **Notifications** subsection of the application web interface window.

The table of rules for sending notifications contains the following information:

- **Type** is the type of rule for sending notifications.

  The following types of rules are possible:

  - **Detections** is a rule for sending a notification about detections.
  - **Component health** is a rule for sending a notification about the operation of application components.
- **Subject**—Subject of the message containing the notification.
- **To**—Email addresses to which the notifications are sent.
- **State**—Status of the rule for sending a notification.

Creating a rule for sending notifications about alerts

To create a rule for sending notifications about alerts:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. Click **Add**.

   This opens the **New rule** window.

4. In the **To** field, enter one or multiple email addresses to which you want to send notifications.

   You can enter several email addresses if you separate them with commas.

5. In the **Subject** field, enter the subject of the notification message.

6. If you want the program to insert the alert importance into the message subject, add the `%importance%` macro to the **Subject** field.

7. In the **Notification type** field, select **Alerts**.

8. In the **Alert importance** drop-down list, select the minimum alert importance for which you want notifications to be sent.

   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.

9. In the **Source or destination** field, enter an IP address and network mask if you want to send notifications about alerts associated with a specific source or destination IP address or subnet address.

10. In the **Email** field, enter an email address if you want to send notifications about alerts associated with a specific email sender or recipient address.

11. Under **Components**, select check boxes next to the names of one or multiple technologies if you want to send notifications about alerts generated by specific technologies.

12. Click **Add**.

The rule for sending notifications about alerts will be added to the list of rules. To send notifications to the specified email address, you must enable the notification rule. Notifications are sent once to each of the email addresses configured for this rule.

Users with the **Administrator** and **Security auditor** roles cannot create rules for sending alert notifications.

In distributed solution mode, you must create notifications separately for each subordinate server (*Secondary Central Node*, *SCN*).

Creating a rule for sending notifications about the operation of program components

To create a rule for sending notifications about the operation of program components:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.

2. Go to the **Notification rules** tab.

3. Click **Add**.

   This opens the **New rule** window.

4. In the **To** field, enter one or multiple email addresses to which you want to send notifications.

   You can enter several email addresses if you separate them with commas.

5. In the **Subject** field, enter the subject of the notification message.

6. If you want the program to insert the alert importance into the message subject, add the `%importance%` macro to the **Subject** field.

7. In the **Notification type** field, select **Program operation**.

8. Under **Components**, select check boxes next to the names of the program's functional areas for which you want to receive notifications.

9. Click **Add**.

The rule for sending notifications about the operation of program components will be added to the list of rules. To send notifications to the specified email address, you must enable the notification rule. Notifications are sent once to each of the email addresses configured for this rule.

Users with the **Security auditor** role cannot create rules for sending notifications about program operation.

In distributed solution mode, notifications are configured separately for each subordinate server (*Secondary Central Node*, *SCN*).

Enabling and disabling a rule for sending notifications

To enable or disable a rule for sending notifications about alerts:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.

2. Go to the **Notification rules** tab.

3. In the **State** column, enable or disable the rule for sending notifications using the toggle switch next to the rule.

   The state of the rule for sending notifications about alerts will be modified.

Users with the **Security auditor** role cannot enable or disable notification rules.

Modifying a rule for sending notifications

To modify a rule for sending notifications:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. In the list of rules for sending notifications, select the rule that you want to modify.
   This opens the **Edit rule** window.
4. Make the relevant changes.
5. Click **Save**.

The rule for sending notifications will be modified.

Users with the **Security auditor** role cannot modify rules for sending notifications.

Deleting a rule for sending notifications

To delete a rule for sending notifications:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. 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.
4. Click **Delete** in the lower part of the window.
5. In the confirmation window, click **Yes**.

The selected rules will be deleted.

Users with the **Security auditor** role cannot delete rules for sending notifications.

Filtering and searching notification forwarding rules by rule type

To filter or search notification rules by rule type:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. Click the ⬚ icon in the table of rules for sending notifications.
   This opens the filter configuration window.
4. 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 rules by notification subject:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. Click the **Subject** link to open the filter configuration window.
4. Enter one or several characters of the notification subject.
5. 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 rules by destination email address:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. Click the **To** link to open the filter configuration window.
4. Enter one or several characters of the email address.
5. 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 rules by status:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. Click the **State** link to open the filter configuration window.
4. Select one or several check boxes next to the values of statuses:
   - **Enabled**
   - **Disabled**
5. 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 the notification rule filter for one or more filtering criteria:

1. In the main window of the program web interface, select the **Settings** section, **Notifications** subsection.
2. Go to the **Notification rules** tab.
3. Click to the right of the header of the column in the notification forwarding rules table 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 Kaspersky Endpoint Agent for Windows

Kaspersky Endpoint Agent is an application that is installed on individual devices within an organization's IT infrastructure. The application constantly monitors the processes running on these devices, as well as open network connections and files modifications. Kaspersky Endpoint Agent interacts with other Kaspersky solutions to detect comprehensive threats (such as targeted attacks).

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.

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 a 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 a previous version, make sure that the following conditions are met:

- The device complies with the hardware and software requirements.
- You have the permissions required to install the application.

If any of these conditions is not met, the corresponding notification will be 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.
- 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. Before you do so, first place the install_props.json file in the same folder as the endpointagent.msi file.

Installing and uninstalling Kaspersky Endpoint Agent locally

This section contains information on how to install Kaspersky Endpoint Agent locally on a device.

Installing Kaspersky Endpoint Agent using the Installation Wizard

The interface of the Installation Wizard application 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 that 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:

- **Restore** damaged application modules.
- **Uninstall** the application from the device.

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, the wizard is launched. As a result of its operation, all application components will be 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 quiet mode with default settings is shown below. After starting the application installation in quiet mode, your participation in the installation process is not required.

Installing Kaspersky Endpoint Agent in quiet mode requires acceptance of the terms and conditions of the 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 USE_AZURE_SUPPORT=1 /qn
```

Command parameters for installing Kaspersky Endpoint Agent

Parameter	Description
`EULA`	Required parameter. This parameter indicates whether the user consents to or declines the terms of the End User License Agreement. Values: • 0 – decline; • 1 – consent. If the value 0 is passed, the application is not installed.
`PRIVACYPOLICY`	Required parameter. This parameter indicates whether the user consents or declines the terms of the Privacy Policy. Values: • 0 – decline; • 1 – consent. If the value 0 is passed, the application is not installed.
`USE_AZURE_SUPPORT`	This parameter sets the flag for using the hardware identifier in the form of the value of the `EnableAzureSupport` HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment parameter for operating systems on an x86 platform or the HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\SOYUZ\4.0\Environment parameter for operating systems on an x64 platform. Values: • 0 – When sending events to the telemetry collection server, Kaspersky Endpoint Agent passes the host's OS identifier from the registry as the sensor_id value in requests to the server. Default value • 1 – When sending events to the telemetry collection server, Kaspersky Endpoint Agent passes the host's BIOS identifier as the sensor_id value in requests to the server.

Repairing Kaspersky Endpoint Agent

An example of restoring the application in quiet mode is shown below. After starting application restoration in 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 quiet mode is shown below. After starting application uninstallation in quiet mode, your participation in the uninstallation process is not required.

Example:
```
msiexec /i {BB66A7B5-A5C0-45E6-92B9-D0B848B6F394} REMOVE=ALL /qn
```
If the application is password protected:
```
msiexec /i {BB66A7B5-A5C0-45E6-92B9-D0B848B6F394} 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.

Installing Kaspersky Endpoint Agent using Kaspersky Security Center

Kaspersky Endpoint Agent can be installed using a remote installation task in Kaspersky Security Center. Installation consists of the following steps:

1. Creating an installation package.
2. Creating a remote installation task.

Kaspersky Security Center also supports other methods of installing applications on groups of managed devices. For more information about installation using a remote installation task and other installation methods, refer to the *Kaspersky Security Center Help*.

When creating an installation package using Kaspersky Security Center 12 and later in order to install Kaspersky Endpoint Agent on devices running Windows XP, use the installation startup file (setup.exe) from the installation package created using Kaspersky Security Center 10.5.

Creating Kaspersky Endpoint Agent installation package

An *installation package* is a set of files generated for the remote installation of a Kaspersky application using Kaspersky Security Center. The installation package contains the required settings to install the application and ensure its operation immediately after installation. The installation package is created on the basis of the file with the KUD extension included in the application distribution package.

Creating an installation package in the Administration Console.

To create an installation package:

1. In the Administration Console, select **Administration Server** → **Advanced** → **Remote installation** → **Installation packages**.
2. Click the **Additional actions** button and select **View current versions of Kaspersky applications** from the drop-down list.

   The list of current versions of Kaspersky applications will be displayed.
3. Select Kaspersky Endpoint Agent installation package.

4. Click the **Download application and create an installation package** button.

   The installation package will be displayed in the list of installation packages.

5. To change the installation package properties, in the context menu of the installation package, select **Properties**.

   The properties window of Kaspersky Endpoint Agent installation package opens. You can specify:

   - Application installation folder
   - Value of the repair mode flag
   - Value of the flag indicating compatibility with Azure WVD
   - The settings of the key file for activating the application

The new installation package is available in the list of installation packages. You can use this installation package for a remote installation task.

Creating an installation package in the Web Console and in the Cloud Console.

To create an installation package:

1. In the main Web Console window, select **Discovery and Deployment** → **Deployment and Assignment** → **Installation packages**.

   The list of installation packages downloaded to Kaspersky Security Center will open.

2. Click the **Add** button.

   The New Package Wizard will start.

3. On the first screen of the wizard, select **Create installation package for Kaspersky application**.

   A list of installation packages available on Kaspersky web servers will be displayed. The list only contains installation packages for applications that are compatible with the current version of Kaspersky Security Center.

4. Select Kaspersky Endpoint Agent installation package.

   This opens a window containing information about the installation package.

5. Read the information and click **Download and create installation package**.

   If the distribution package cannot be converted to an installation package, the **Download distribution package** button will be displayed instead of the **Download and create installation package** button. In that case, do the following:

   a. Click the **Download distribution package** button to download the distribution package to your computer.

      Wait for the download to finish.

   b. Close the installation package creation wizard window and restart the wizard.

   c. On the first page of the wizard, select **Create installation package from file**.

   d. On the second page of the wizard, specify the path to the distribution package file on your computer.

   e. Follow the wizard's instructions.

6. When you create the installation package, accept the terms and conditions of the License Agreement and the Privacy Policy.

7. After download is complete, click **Close**.

   The selected installation package has been downloaded to the Administration Server shared folder, into the Packages subfolder. The downloaded installation package will be displayed in the list of installation packages.

8. To change the installation package's properties, click on the installation package name.

   The properties window of Kaspersky Endpoint Agent installation package opens. You can specify:

   - Application installation folder
   - Value of the repair mode flag
   - Value of the flag indicating compatibility with Azure WVD
   - The settings of the key file for activating the application

The new installation package is available in the list of installation packages. You can use this installation package for a remote installation task.

When creating an installation package using Kaspersky Security Center 12 and later in order to install Kaspersky Endpoint Agent on devices running Windows XP, use the installation startup file (setup.exe) from the installation package created using Kaspersky Security Center 10.5.

Creating Kaspersky Endpoint Agent remote installation task

The Remote application installation task is intended for the remote installation of Kaspersky Endpoint Agent using Kaspersky Security Center. To install the application, the task uses the application installation package.

Creating a remote installation task in the Administration Console.

To create a remote installation task:

1. In the Administration Console, open the **Administration Server** → **Tasks** folder.

   A list of tasks appears.

2. Click **Create a task**.

   The task creation wizard will start. Follow its steps.

Step 1. Selecting the task type

Select **Kaspersky Security Center Administration Server** → **Remote application installation**.

Step 2. Selecting the installation package

In the list of installation packages, select Kaspersky Endpoint Agent installation package.

You can change the properties of the Kaspersky Security Center installation package.

Step 3. Optional

The Network Agent can be installed together with Kaspersky Endpoint Agent. The Network Agent provides interaction between the Administration Server and the client computer. If the Network Agent is already installed on the computer, it is not re-installed.

If you want to install the Network Agent together with Kaspersky Endpoint Agent, select the Network Agent installation package.

Step 4. Settings

Configure the following additional application settings:

- **Force installation package download**. Select the application installation method:
  - **Using Network Agent**. If the Network Agent is not installed on the computer, first the Network Agent is installed using the operating system tools. Than Kaspersky Endpoint Agent is installed using the Network Agent tools.
  - **Using operating system resources through distribution points**. The installation package will be disseminated to client computers through distribution points using operating system resources . You can select this option if there is at least one distribution point in your network. For details on distribution point operation, refer to *Kaspersky Security Center Help*.
  - **Using operating system resources through Administration Server**. The Administration Server disseminates files to client computers by means of the operating system. This option can be selected if the Network Agent is not installed on the client computer, but the client computer is in the same network as the Administration Server.
- **Behavior of devices managed by other Servers**. Select how to install Kaspersky Endpoint Agent. If more than one Administration Server is installed in the network, these Administration Servers can detect the same client computers. It can result in remote installation of the same application on one client computer from several Administration Servers and in other conflicts.
- **Do not install application if it is already installed**. Clear this check box if you want, for example, to install an earlier version of the application.

Step 5. Selecting how to restart the operating system

Select the action to be performed if the computer must be restarted.

Step 6. Selecting devices to receive the task assignment

Select the devices on which Kaspersky Endpoint Agent will be installed.

Step 7. Selecting an account to run the task

Select an account to install the Network Agent using the operating system. In this case, administrator permissions are required to access the computer. You can add multiple accounts. If an account does not have the required permissions, the installation wizard uses the next account in the list. You do not need to select an account to install Kaspersky Endpoint Agent using the Network Agent.

Step 8. Configuring task schedule settings

Configure the task start schedule. For example, manually or when the computer is idle.

Step 9. Defining the task name

Enter the task name, for example, `Installing Kaspersky Endpoint Agent`.

Step 10. Finishing task creation

Complete the wizard operation. If required, select the **Run task after wizard finishes** check box. You can monitor the task's progress in the task properties. The application will be installed in quiet mode.

Creating a remote installation task in the Web Console and in the Cloud Console.

To create a remote installation task:

1. In the main Web Console window, select **Devices** → **Tasks**.

   A list of tasks appears.

2. Click the **Add** button.

   The task creation wizard will start. Follow its steps.

Step 1. Configuring the general task settings

In order to configure the general task settings:

1. In the **Application** drop-down list, select **Kaspersky Security Center**.
2. In the **Task type** drop-down list, select **Remote application installation**.
3. In the **Task name** field, enter a short description, for example, `Installing Kaspersky Endpoint Agent`.
4. In the **Devices to which the task will be assigned** section, select the task scope.

Step 2. Selecting computers for installation

At this step, select the computers on which Kaspersky Endpoint Agent will be installed in accordance with the selected task scope.

Step 3. Configuring the installation package settings

At this step, configure the installation package settings:

1. Select Kaspersky Endpoint Agent installation package.
2. Select the Network Agent installation package.

   The selected version of the Network Agent will be installed together with Kaspersky Endpoint Agent. The Network Agent provides interaction between the Administration Server and the client computer. If the Network Agent is already installed on the computer, it is not re-installed.

3. In the **Force installation package download** section, select the application installation method:

   - **Using Network Agent**. If the Network Agent is not installed on the computer, first the Network Agent is installed using the operating system tools. Than Kaspersky Endpoint Agent is installed using the Network Agent tools.

   - **Using operating system resources through distribution points**. The installation package will be disseminated to managed devices through distribution points using operating system resources. You can select this option if there is at least one distribution point in your network. For details on distribution point operation, refer to *Kaspersky Security Center Help*.

   - **Using operating system resources through Administration Server**. The Administration Server will deliver files to managed devices by means of the operating system. This option can be selected if the Network Agent is not installed on the managed device, but the managed device is in the same network as the Administration Server.

4. In the **Maximum number of concurrent downloads** field, specify the limit on the number of installation package download requests to the Administration Server. A limit on the number of requests helps prevent network overload.

5. In the **Number of installation attempts** field, specify the limit on the number of application installation attempts. After successfully installing Kaspersky Endpoint Agent , the task will automatically start the next installation.

6. If required, clear the **Do not install application if it is already installed** check box. This will allow, for example, installing an earlier version of the application.

7. If required, clear the **Verify operating system type before downloading** check box. This will prevent the superfluous download of the application distribution package in the event that the computer's operating system does not meet the software requirements. If you are sure that the computer's operating system meets the software requirements, you can skip this check.

8. If required, select the **Assign package installation in Active Directory group policies** check box. Kaspersky Endpoint Agent can be installed manually using the Network Agent or Active Directory. To install using the Network Agent, the remote installation task must be started with the domain administrator permissions.

9. If required, select the **Prompt the user to close running applications** check box. Installing Kaspersky Endpoint Agent requires computer resources. For the user's convenience, the application installation wizard prompts the user to close running applications before starting the installation. This will prevent slowdowns in the operation of other applications, as well as possible computer malfunctions.

10. In the **Behavior of devices managed by other Servers** section, select the installation method for Kaspersky Endpoint Agent. If more than one Administration Server is installed in the network, these Administration Servers can detect the same client computers. It can result in remote installation of the same application on one client computer from several Administration Servers and in other conflicts.

Step 4. Selecting how to restart the operating system

Select the action to be performed if the computer must be restarted.

Step 5. Selecting an account to run the task

Select an account to install the Network Agent using the operating system. In this case, administrator permissions are required to access the computer. You can add multiple accounts. If an account does not have the required permissions, the installation wizard uses the next account in the list. You do not need to select an account to install Kaspersky Endpoint Agent using the Network Agent.

Step 6. Finishing task creation

Complete the wizard's operation by clicking the **Finish** button. The new task will appear in the task list. To run the task, select the check box next to the task and click **Run**. The application will be installed in quiet mode.

Installing Kaspersky Endpoint Agent administration tools

This section contains information on how to install Kaspersky Endpoint Agent Management plug-in for managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console or Kaspersky Endpoint Agent Management web plug-in for managing Kaspersky Endpoint Agent using Kaspersky Security Center Web Console.

Installing and updating Kaspersky Endpoint Agent Management plug-in

The Kaspersky Endpoint Agent Management plug-in must be installed in order to manage Kaspersky Endpoint Agent using the Kaspersky Security Center Administration Console.

To install the Kaspersky Endpoint Agent Management plug-in,

copy the klcfginst.msi file from the distribution kit to the device on which Kaspersky Security Center Administration Console is installed and run the file.

The application Installation Wizard starts.

Updating a previously installed version of the Kaspersky Endpoint Agent Management plug-in

This update is only available for the Kaspersky Endpoint Agent Management plug-in versions 3.7 and later.

When installing a plug-in on a device with a previous plug-in version:

- All the setting values, including policies, group and local tasks, are migrated to the new plug-in version, and the previously installed plug-in version is automatically removed.
- The Kaspersky Endpoint Agent settings that were not available in the previous plug-in version are set to default values and can be configured.

  To apply previously unavailable settings, after updating the plug-in, change the desired policy or task and save your changes.

- Policy templates created in the previous plug-in version are available in the new plug-in version.

You can use the new plug-in to manage previous Kaspersky Endpoint Agent versions. However, previous versions of Kaspersky Endpoint Agent do not support and do not apply the settings that have appeared in the new plug-in version.

Installing and updating Kaspersky Endpoint Agent Management web plug-in

Kaspersky Endpoint Agent Management web plug-in must be installed to manage Kaspersky Endpoint Agent using Kaspersky Security Center Web Console.

You can install the web plug-in in one of the following ways:

- Using the Initial Setup Wizard of the Kaspersky Security Center Web Console.
- From the list of available distribution packages in the Kaspersky Security Center Web Console.

  For detailed information on installing management web plug-ins, refer to the Kaspersky Security Center Help.

- By downloading the distribution package to the Kaspersky Security Center Web Console from a third-party source.

  To install the web plug-in, add a ZIP archive with the distribution package of the Kaspersky Endpoint Agent web plug-in to the Web Console interface (Console settings → Web plug-ins). You can download the web plug-in distribution kit, for example, from Kaspersky's website.

Updating a previously installed version of the Kaspersky Endpoint Agent Management web plug-in

When installing a plug-in on a device with a previous plug-in version:

- All the setting values, including policies, group and local tasks, are migrated to the new plug-in version, and the previously installed plug-in version is automatically removed.
- The Kaspersky Endpoint Agent settings that were not available in the previous plug-in version are set to default values and can be configured.

  > To apply previously unavailable settings, after updating the plug-in, change the desired policy or task and save your changes.

- Policy templates created in the previous plug-in version are available in the new plug-in version.

You can use the new plug-in to manage previous Kaspersky Endpoint Agent versions. However, previous versions of Kaspersky Endpoint Agent do not support and do not apply the settings that have appeared in the new plug-in version.

Updating Kaspersky Endpoint Agent from the previous version

Only Kaspersky Endpoint Agent version 3.8 and later can be updated. The update is possible for application versions installed both as part of the Endpoint Protection Platform application and independently. The update can be performed by installing the new version.

When you update Kaspersky Endpoint Agent, the current license is automatically applied to Kaspersky Endpoint Agent. The license term will remain unchanged. When updating the application with an expired license, the new application version works in limited functionality mode after installation.

If the license for the updated version has expired, you can add the license key during the update. The key file can be passed using one of the specified methods.

When Kaspersky Endpoint Agent is installed on a device with a previous version of Kaspersky Endpoint Agent, first all data that can be migrated is saved and used, then the previous version of the application is automatically uninstalled.

If Kaspersky Endpoint Agent is installed on a device with a previous version of Kaspersky Endpoint Agent, you will need to create an account to connect to Kaspersky Security Center and migrate data from the previous version. The account uses the default name: AutoIOC_Admin and a password specified by the user.

When updating a previous version of Kaspersky Endpoint Agent that is password protected, you must pass this password to the installer in 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 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.

When updating Kaspersky Endpoint Agent as part of EPP, you can pass the password as the value of the `UNLOCK_PASSWORD` key in the install_props.json configuration file.

The application password passed through the install_props.json configuration file is stored in the file in non-encrypted form. To reduce the probability of unauthorized access to this data, it is recommended to restrict access to the install_props.json file and delete it from the device after installing or updating the application.

Starting from version 3.10, Kaspersky Managed Protection (also referred to as KMP) usage cannot be configured by means of Kaspersky Endpoint Agent. If usage of the KMP service was enabled in the previous Kaspersky Endpoint Agent version, the KMP service continues functioning after the application is updated to version 3.10 and later. After the application update, you can disable the KMP service only using Kaspersky Endpoint Agent Administration Plug-in or Kaspersky Endpoint Agent Web Plug-in of versions earlier then 3.10.

When installing a plug-in on a device with a previous plug-in version:

- All the setting values, including policies, group and local tasks, are migrated to the new plug-in version, and the previously installed plug-in version is automatically removed.
- The Kaspersky Endpoint Agent settings that were not available in the previous plug-in version are set to default values and can be configured.

  To apply previously unavailable settings, after updating the plug-in, change the desired policy or task and save your changes.

- Policy templates created in the previous plug-in version are available in the new plug-in version.

You can use the new plug-in to manage previous Kaspersky Endpoint Agent versions. However, previous versions of Kaspersky Endpoint Agent do not support and do not apply the settings that have appeared in the new plug-in version.

Repairing Kaspersky Endpoint Agent

If you launch Kaspersky Endpoint Agent installer in Repair mode, it will check and restore the integrity of all damaged application modules and system registry keys created during the application's installation.

You can run the installer in 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 Repair mode and *the application does not need to be repaired*, the installer will not perform any changes on the device.

If Kaspersky Endpoint Agent installer is launched in Repair mode and *the application is not installed on the device*, the application installation will start.

If Kaspersky Endpoint Agent installer is launched in 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

The Windows Installer service performs the following changes on the protected device during the installation of Kaspersky Endpoint Agent:

- 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:
  - On a 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\
  - On a 64-bit version of Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\
- Folder containing Kaspersky Endpoint Agent (x86) drivers:
  - On a 32-bit version of Microsoft Windows: %ProgramFiles%\Kaspersky Lab\Endpoint Agent\drivers\<OS version>\<driver name>
  - On a 64-bit version of Microsoft Windows: %ProgramFiles (x86)%\Kaspersky Lab\Endpoint Agent\drivers\x64\<OS version>\<driver name>
- Folders containing IOC files:
  - In 32-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
  - In 64-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
- 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\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\Data\killchain
    - %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's 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 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's 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 facilitates the interaction between Kaspersky Endpoint Agent and the Central Node component.
- ANGARA.dll (executed in proton.exe) is a service that facilitates the 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.

  When installed on a device running Microsoft Windows XP, the klncapxp.sys driver is registered instead of klncap.sys.

System registry keys

As a result of Kaspersky Endpoint Agent's installation, the following registry keys are created:

Registry keys are listed in the 32-bit application view.

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdDispl
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\ProdVersi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\NagentMi
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\SOYUZ\4.0.0.0\Connecto
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\UninstallString
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\SOYUZ\4.0.0.0\Installer\ProductCode
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\NoPPL]

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\BFESDDL]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Enable]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\CrashDump\Folder]
- [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\Environment\EnableKillChain]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\SvmUpdateMode]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\MsiPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\AgentPath]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Environment\EventsExpirationTimeout]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallTime]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLCID]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Install\InstallLocalization]
- [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]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\SOYUZ\4.0\Trace\Configuration(Example)]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\StartMenu]
- [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\Ksn]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\Kmp]
- [HKEY_CURRENT_USER\Software\KasperskyLab\SOYUZ\ProductUrl]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\angara]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncap]

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klncapxp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klsnsr]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vostok]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\soyuz]

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 installation:
  - By specifying the key file at a certain step of the Installation Wizard.
  - By placing the key file in the same folder as the endpointagent.msi file before starting the installation in quiet mode (including remote installation).
  - By specifying the path to the key file using the `LICENSEKEYPATH` parameter when installing the application in 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 to activate Kaspersky Endpoint Agent, the application will be installed without being activated.

When you update Kaspersky Endpoint Agent, the current license is automatically applied to Kaspersky Endpoint Agent. The license term will remain unchanged. When updating the application with an expired license, the new application version works in limited functionality mode after installation.

If the license for the updated version has expired, you can add the license key during the update. The key file can be passed using one of the specified methods.

- After installation:
  - Using the Application activation task in Kaspersky Security Center Administration Console or in Kaspersky Security Center Web Console.
  - Using the command line locally on the device.

You can use Kaspersky Security Center as a proxy server to activate Kaspersky Endpoint Agent.

You can view information about the current Kaspersky Security Center license in the **Kaspersky licenses** section, in the device properties, or using the command line.

For detailed information on managing keys using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

After the license expires, the application will continue to work but with limited functionality.

Functional limitations after the license expiration

When the license expires, the following limitations will arise in the operation of Kaspersky Endpoint Agent functional components:

- Telemetry data is not collected.
- Network isolation cannot be enabled.

  If network isolation was enabled when the license expired, the application will disable 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 will stop blocking objects that fall under the specified Execution prevention rules.
- The following tasks stop and cannot be started: Run process, Terminate process, Delete file.
- The Standard IOC Scan tasks will 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 will create the critical `LicenseViolation` event in the Windows event log and in the Kaspersky Security Center Administration Server log. When working using the command line, the application will return the 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 keys using Kaspersky Security Center, refer to *Kaspersky Security Center Help*.

To view information about an active license in the Kaspersky Security Center Administration Console:

1. 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.
2. In the workspace, select the **Devices** tab.
3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
4. Select **Properties** in the device context menu.

   The device properties window opens.
5. Select the **Applications** section.

   A list of Kaspersky applications installed on the device is displayed in the window.
6. 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.
7. Select the **Keys** section.

Information about the current license will be displayed in the window.

To view information about an active license in the Kaspersky Security Center Web Console:

1. On the **Devices** tab, select **Managed devices**.
2. Click the name of the device you want.
3. In the device properties window that opens, select the **Applications** tab.
4. In the list of applications, select **Kaspersky Endpoint Agent**.
5. In the application properties window that opens, select the **General** tab and open the **License** section.

The general information about active and backup license keys will be displayed.

Managing Kaspersky Endpoint Agent using Kaspersky Security Center Administration Console

Kaspersky Security Center provides a centralized solution for the main tasks of managing and maintaining an 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 the administrator to configure all the components of protection built based on Kaspersky applications.

Kaspersky Security Center enables the remote installation, uninstallation, starting and stopping of Kaspersky Endpoint Agent, as well as configuration of the application settings, as well as the starting and stopping of application tasks. Kaspersky Security Center offers 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*.

Kaspersky Security Center Administration Console (hereinafter also referred to as *Administration Console*) provides the user interface for working with Kaspersky Security Center. Administration Console is implemented as an extension component to the Microsoft Management Console (MMC).

Kaspersky Endpoint Agent can be managed in Kaspersky Security Center Administration Console using the 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 policies and enable policy settings.

Creating Kaspersky Endpoint Agent policy

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Selecting an application for creating a group policy** window, select Kaspersky Endpoint Agent.
5. Click **Next**.

6. 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:

      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**.

7. In the **New policy** window, select one of the following options:

   - **Create a new policy and configure its settings**.
   - **Create a new policy with default settings**.

   If you enabled the **Use the policy settings for previous application version** setting at the previous step, the **Create a new policy and configure its 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, which shows if the policy is applied, depends on the position of the switches in the groups of settings of the imported policy.

8. Click **Next**.

9. In the **Select policy type** window, select the required Kaspersky Endpoint Agent deployment method:

   - **Integration with Kaspersky Sandbox**
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks**

10. Click **Next**.

11. If you select the **Create a new policy and configure its settings** option, perform one of the following actions in all sequentially displayed settings windows:

    - To configure the application settings in the displayed sections during 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 during the previous step and may differ from the one described.

- Configuring integration between Kaspersky Endpoint Agent and Kaspersky Sandbox.
- Configuring integration of Kaspersky Endpoint Agent with Endpoint Detection and Response Expert (KATA EDR) and Kaspersky Industrial CyberSecurity for Networks (KICKS for Networks) components.
- Configuring threat response settings.
- Configuring application repositories.
- Configuring application security settings.
- Configuring general application settings.

12. In the **Target group** window, select the 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 will open.

    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**.

13. In the **Creating a group policy for the application** window, select one of the following policy statuses:

    - **Active policy** to activate the policy as soon as it is created.
    - **Inactive policy** to activate the policy later.
    - **Out-of-office**. The policy becomes active when the computer leaves the corporate network.

14. Select the **Open policy properties after creation** check box if you want to perform additional configuration of the policy immediately after creating it.

15. Click **Finish**.

The created policy will now appear 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. The settings in the policy sections are divided into groups. You can enable either individual groups or all groups 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 **Unaffected by policy** to **Under policy**.

   All the settings of the group will be applied in the policy after the changes are saved.

Configuring Kaspersky Endpoint Agent settings

This section describes how to configure Kaspersky Endpoint Agent settings.

Opening Kaspersky Endpoint Agent settings window

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To open the Kaspersky Endpoint Agent settings window:

1. Open Kaspersky Security Center Administration Console.
2. Expand the **Managed devices** node in the 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, these settings cannot be edited in the **Application settings** window, except for the network isolation settings.

The settings of automatic network isolation can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be configured in the properties of an individual device.

Configuring Kaspersky Endpoint Agent security settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.

Configuring user permissions

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 will open.
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 the check boxes for the items with the desired permissions.
8. Click **OK**.
9. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
10. In the policy properties window, click **OK**.

The user permissions for managing the application settings and services have now been configured and applied.

Enabling Password protection

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Unrestricted user access to the application and its settings can reduce the security level of the device. Password protection is a means 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 a password that satisfies the following requirements:

   - It is at least 8 characters long.
   - It does not contain the user account name.
   - It does not match the name of the device on which Kaspersky Endpoint Agent is installed.
   - It contains characters from at least three of the following groups:
     - uppercase characters (A-Z);
     - lowercase characters (a-z);
     - numbers (0-9);
     - special characters (!$#%).

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

8. Click **OK**.

Password protection is now enabled. If a user attempts to perform a password protected action, the application will prompt 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 login attempts after many attempts of entering an incorrect password.

Enabling and disabling Self-Defense

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The Self-Defense mechanism of Kaspersky Endpoint Agent provides protection from malware that tries to lock or delete the application. The Self-Defense mechanism prevents the 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, enable or disable the **Enable self-defense for application modules in memory** setting.

   The setting is enabled by default.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click **OK**.

The Self-Defense mechanism is now enabled or disabled.

Configuring Kaspersky Endpoint Agent connection settings to a proxy server

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Proxy server connection settings are used for updating databases, activating the application, and external services.

If you want to use a specified proxy server when connecting to KATA server, Kaspersky Sandbox server or Kaspersky Industrial CyberSecurity for Networks server, make sure that the **Connect using the proxy server if specified in the general settings** option is selected when configuring integration with KATA, Kaspersky Industrial CyberSecurity for Networks or Kaspersky Sandbox. This option is not selected by default.

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 **General settings** subsection.
5. Select one of the following proxy service usage options:
   - **Do not use proxy server**.
   - **Automatically detect proxy server address.**
   - **Use proxy server with specified settings**.
6. If you select the **Automatically detect proxy server address** option, the proxy server for further telemetry transmission will be detected automatically.
7. 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.
8. If you want to use NTLM authentication (NT LAN Manager Network Authentication Protocol) to connect 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.
9. 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.

10. Click the **Apply** button.

    As a result, you will return to the policy properties window.

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

12. Click **OK**.

Proxy server connection settings are now configured.

Configuring Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **General 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 **Unaffected by policy** to **Under policy**.

7. Click **OK**.

Kaspersky Security Center usage as a proxy server for Kaspersky Endpoint Agent activation is now enabled.

Configuring KSN usage in Kaspersky Endpoint Agent

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To protect your computer more effectively, Kaspersky Endpoint Security uses data received from users around the globe. Kaspersky Security Network is designed to receive this data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services that provide access to the online Kaspersky Knowledge Base that contains information about the reputations of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by the EPP application 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 parts of files, that may be exploited by intruders to harm the computer or data can be also sent to Kaspersky to be further examined.

No personal data is collected, processed, or stored. The types of data that Kaspersky Endpoint Agent sends to Kaspersky Security Network are described in the KSN Statement.

Participation in Kaspersky Security Network is voluntary. KSN usage is disabled by default. After enabling KSN usage, you can disable this option at any time.

Starting from version 3.10, Kaspersky Managed Protection (also referred to as KMP) usage cannot be configured by means of Kaspersky Endpoint Agent. If usage of the KMP service was enabled in the previous Kaspersky Endpoint Agent version, the KMP service continues functioning after the application is updated to version 3.10 and later. After the application update, you can disable the KMP service only using Kaspersky Endpoint Agent Administration Plug-in or Kaspersky Endpoint Agent Web Plug-in of versions earlier then 3.10.

To enable KSN 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 **Kaspersky Security Network** 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, understood, and accept the terms and conditions of this Kaspersky Security Network Statement** check box.
7. Select the **Enable Kaspersky Security Network usage** check box.

8. If you want to use Kaspersky Security Center for telemetry transmission, select the **Use Kaspersky Security Center as a KSN proxy server** check box.

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

10. Click **OK**.

KSN usage is enabled.

Configuring integration between Kaspersky Endpoint Agent and KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure integration between Kaspersky Endpoint Agent and the KATA Central Node component using the Kaspersky Security Center Administration Console.

Configuring data submission settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Telemetry collection servers** section, select the **General settings** subsection.

5. In the **Data submission settings** group, do the following:

   - Specify the value in the **Events transmission period (sec.)** field.
     The default value is 30 seconds.

- Specify the value in the **Maximum number of events in a package** field.

  The default value is 1024 events in a package.

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

Configuring request throttling settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The request throttling feature allows restricting the flow of events with low importance from Kaspersky Endpoint Agent to the Central Node component. Event importance is evaluated by the application.

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 **Telemetry collection servers** section, select the **General settings** subsection.
5. In the **Request throttling** group of settings, you can perform the following actions:
   - Enable or disable the **Enable request throttling** setting.

     The setting is enabled by default.
   - Specify the number of events in the **Maximum number of 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 threshold for the flow of events of the same type with low importance in the **Percentage of event limit excess** 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. You can specify a value from 5% to 100%. The default value is 15%.

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

   The default switch position is **Under policy**.

7. Click **OK**.

Enabling and disabling integration with KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you use Nginx as a proxy server between a device with Kaspersky Endpoint Agent installed and KATA 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 KATA for processing. Otherwise, Nginx will not send objects whose size exceeds the specified value. The default value is 1 MB.

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 **Telemetry collection servers** section, select the **Integration with KATA** subsection.
5. In the **Connection settings** group, do one of the following:
   - To enable integration with KATA Central Node:
     a. Select the **Enable KATA integration** check box.
     b. In the **List of KATA servers** settings group, for one or more KATA servers, specify the IP address or full domain name of the KATA server, as well as the port for connecting to the server.

        Kaspersky Endpoint Agent connects to the first server in the list. If the connection does not succeed, Kaspersky Endpoint Agent connects to the second server and so on down the list.
   - To disable integration with KATA Central Node, clear the **Enable KATA integration** check box.
6. In the **Connection settings** group, enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to the KATA server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to the KATA server.

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

Integration with KATA Central Node is enabled or disabled.

Configuring trusted connection with KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection between Kaspersky Endpoint Agent and KATA Central Node, perform the following actions 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 **Telemetry collection servers** section, select the **Integration with KATA** subsection.
5. In the **Connection settings** group, select the **Use pinned certificate to protect 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 the **Add** button.
   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 the 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 **Unaffected by policy** to **Under policy**.

12. Click **OK**.

The trusted connection to KATA server is now configured.

Configuring synchronization settings between Kaspersky Endpoint Agent and KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Telemetry collection servers** section, select the **Integration with KATA** subsection.

5. In the **Connection settings** group, configure the following settings:

    - **Timeout (sec.)**. Specify the maximum KATA server response timeout. The default value is 10 seconds.
    - **Send synchronization 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. The default value is 5 minutes.

- Select or clear the **Use TTL period when sending events** check box. The check box is cleared by default.

  If the check box is selected, Kaspersky Endpoint Agent does not send information about the processes that are started again to the KATA server. Kaspersky Endpoint Agent does not consider the launch of the process as repeated if the process is started after the end of the TTL period.

- If you select the **Use TTL period when sending events** check box, specify the time in the **TTL period (min.)** field. The default value is 1440 minutes.

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

7. Click **OK**.

Configuring EDR telemetry settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure:

- Exclusions for EDR telemetry about application processes, which Kaspersky Endpoint Agent processes and sends to a server with the KATA Central Node or Kaspersky Industrial CyberSecurity for Networks component.
- Optimization of the volume of EDR telemetry that Kaspersky Endpoint Agent processes and sends to a server with the Kaspersky Industrial CyberSecurity for Networks component.
- Exclusions for EDR telemetry about network communications, which Kaspersky Endpoint Agent processes and sends to a server with the Kaspersky Industrial CyberSecurity for Networks component.

Enabling and configuring exclusions for and optimization of sent EDR telemetry about application processes

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure exclusions for and optimization of the volume of EDR telemetry about application processes using Kaspersky Security Center Administration Console, in the properties of an individual device or in the policy settings for a group of devices.

Exclusions for EDR telemetry about application processes are available when Kaspersky Endpoint Agent is integrated with servers where KATA Central Node or Kaspersky Industrial CyberSecurity for Networks is installed.

Kaspersky Endpoint Agent does not analyze or send data on excluded application processes to the server with KATA Central Node or Kaspersky Industrial CyberSecurity for Networks installed.

Optimization of the volume of EDR telemetry about application processes can be managed (enabled / disabled) when Kaspersky Endpoint Agent is integrated with servers where Kaspersky Industrial CyberSecurity for Networks is installed.

If optimization of the volume of EDR telemtry is enabled, Kaspersky Endpoint Agent does not send events with 102 (basic communications) and 8 (network activity of a process) codes for the Microsoft SMB protocol and the Network Agent process klnagent.exe regarding processes of applications on a server where Kaspersky Industrial CyberSecurity for Networks is installed.

To enable and configure exclusions for and optimization of the volume of EDR telemetry on application processes:

1. Do one of the following:

- **Open the application properties window for an individual device**.

    1. 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.
    2. In the workspace, select the **Devices** tab.
    3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
    4. Select **Properties** in the device context menu.

       The device properties window opens.
    5. Select the **Applications** section.

       A list of Kaspersky applications installed on the device is displayed in the window.
    6. 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. Select the **EDR telemetry → Excluded processes** section.

3. In the **Exclusions** settings group, enable the **Use exclusions** setting to enable use of EDR telemetry exclusions.

4. Configure optimization of the volume of EDR telemetry:

> When Kaspersky Endpoint Agent is integrated with servers where KATA Central Node is installed, optimization of the volume of EDR telemetry should always be enabled.

- Disable the **Optimize the amount of telemetry** setting if you want Kaspersky Endpoint Agent to send events with codes 102 (basic communications) and 8 (the process's network activity) for the Microsoft SMB protocol, WinRM service, and the Network Agent process klnagent.exe.
- Enable the **Optimize the amount of telemetry** setting if you want Kaspersky Endpoint Agent to not send events with codes 102 (basic communications) and 8 (the process's network activity) for the Microsoft SMB protocol and the Network Agent process klnagent.exe.

> If the **Use exclusions** setting is disabled, Kaspersky Endpoint Agent does not send events with codes 102 (basic communications) and 8 (the process's network activity) for the Microsoft SMB protocol and the Network Agent process klnagent.exe, regardless of the value of the **Optimize the amount of telemetry** setting.

5. Create a list of exclusions:

   a. Click the **Add** button.

   b. In the **Rule properties** window that opens, **configure the exclusion settings**:

   > Exclusion settings are applied using a logical AND.

   To create an exclusion, specify the value in the **Full path** field and select at least one event type in the **Use this exclusion for the following event types** list.

   > If the **Network events** value is selected for the **Use this exclusion for the following event types** criterion, specify the full path to the file in the **Full path** field.

   > The object for which you create an exclusion must be available on the protected device at the time the exclusion settings are applied. For example, if you first configure exclusion for a specific application, and then install that application on the protected device, this exclusion will not be applied.

   1. In the **Process information** section, specify the values in the following fields:

      - **Full path**. Full path to the file, including its name and extension. You can use file masks (using the ? and * characters), as well as system environment variables.
      - **Command line text**. Command line to run the object.
      - **Parent folder path**. The path to the folder where the file is located.

2. In the **File properties** section, specify the values in the following fields:

   - **File description**. The value of the FileDescription parameter from the resource of the RT_VERSION type (VersionInfo).
   - **Original file name**. The value of the OriginalFilename parameter from the resource of the RT_VERSION type (VersionInfo).
   - **File version**. The value of the FileVersion parameter from the resource of the RT_VERSION type (VersionInfo).

3. In the **File checksums** section, specify the values in the following fields:

   - **MD5**. MD5 hash of the file.
   - **SHA256**. SHA256 hash of the file.

4. In the **Use this exclusion for the following event types** list, select at least one value:

   - **File modification**.
   - **Network events**.
   - **Interactive input in the console**.

     This event type is selected by default.
   - **Loading the process module**.
   - **Changes in the Registry**.

c. Click **OK** to save the changes and close the **Rule properties** window.

   The new exclusion is created and displayed in the list of exclusions.

d. If you need to export the exclusion list to an XML file, click the **Export** button.

e. If you need to import the exclusion list from an XML file, click the **Import** button.

f. If you need to modify an exclusion, click the **Modify** button.

g. If you need to delete an exclusion from the list, select the exclusion and click the **Delete** button.

6. If you are configuring the policy settings, make sure that the switch in the upper right corner of the group of settings is turned on. It is the default position of the switch.

7. Click **OK** to save the changes.

Enabling and configuring exclusions for sent EDR telemetry about network communications

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure exclusions for EDR telemetry using Kaspersky Security Center Administration Console, in the properties of an individual device or in the policy settings for a group of devices.

Exclusions for EDR telemetry about network communications are applied when Kaspersky Endpoint Agent is integrated with servers where Kaspersky Industrial CyberSecurity for Networks is installed.

Kaspersky Endpoint Agent does not analyze or send data matching exclusion settings to the server with KATA Central Node or Kaspersky Industrial CyberSecurity for Networks installed.

To enable and configure EDR telemetry about network communications:

1. Do one of the following:

- **Open the application properties window for an individual device**.

    1. 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.
    2. In the workspace, select the **Devices** tab.
    3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
    4. Select **Properties** in the device context menu.

       The device properties window opens.
    5. Select the **Applications** section.

       A list of Kaspersky applications installed on the device is displayed in the window.
    6. 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. Select the **EDR telemetry → Excluded network communications** section.
3. In the **Exclusions** settings group, enable the **Use exclusions** setting to enable use of EDR telemetry exclusions.

4. Create a list of exclusions:

   a. Click the **Add** button.

   b. In the **Rule properties** window that opens, **configure the exclusion settings.**

   > Exclusion settings are applied using a logical AND.

      1. In the **Name** field, enter the name of the exclusion.
      2. In the **Direction** drop-down list, select the direction of network traffic.
      3. In the **Protocol** drop-down list, select the network protocol.
      4. If you select a custom protocol, in the **Number** field, enter the network protocol number.
      5. Select the **Local port OR range** check box and enter the port number or number range.

         For incoming connections (in the **Direction** drop-down list, **Incoming** is selected), enter the port or range of ports for the local device.

         For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the port or range of ports for the remote device.

         The values 1–65535 are available for port numbers.

         The values 1–10, 20–30000 and 1–65535 are available for a range of ports.

         Limitations:

         - For network connections of a local device running the Windows XP operating system, you can specify only a single port, because Windows XP does not support a range of ports.
         - For network connections of a remote device running the Windows XP operating system, you can specify a range of ports, but only the first port in the specified range is correctly applied, because Windows XP does not support a range of ports.

      6. Select the **Remote port OR range** check box and enter the port number or number range.

         For incoming connections (in the **Direction** drop-down list, **Incoming** is selected), enter the port or range of ports for the remote device.

         For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the port or range of ports for the local device.

         The values 1–65535 are available for port numbers.

         The values 1–10, 20–30000 and 1–65535 are available for a range of ports.

Limitations:

- For network connections of a local device running the Windows XP operating system, you can specify only a single port, because Windows XP does not support a range of ports.
- For network connections of a remote device running the Windows XP operating system, you can specify a range of ports, but only the first port in the specified range is correctly applied, because Windows XP does not support a range of ports.

7. Select the **Local address** check box and enter the network address of the device for which Kaspersky Endpoint Agent will not analyze or send EDR telemetry about network traffic in accordance with the exclusion settings.

   For incoming exclusions (in the **Direction** drop-down list, **Incoming** is selected), enter the network address for the local device.

   For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the network address of the remote device.

   > For IP addresses, only addresses in IPv4 format are supported.

8. Select the **Remote address** check box and enter the network address of the device for which Kaspersky Endpoint Agent will not analyze or send EDR telemetry about network traffic in accordance with the exclusion settings.

   For incoming connections (in the **Direction** drop-down list, **Incoming** is selected), enter the network address for the remote device.

   For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the network address for the local device.

   > For IP addresses, only addresses in IPv4 format are supported.

9. **Create the list of application** for which Kaspersky Endpoint Agent will not analyze or send EDR telemetry about network traffic in accordance with the exclusion settings.

   1. Select the **Applications** check box.
   2. In the field below, specify the path to the executable file of the application you want to add to the list. You can enter the path manually or with the help of the **Browse** button.
   3. Click the **Add** button.
   4. For each application you want to add to the list, repeat steps 2 and 3 of the guide.
   5. If necessary, remove an application from the list:
      a. Select the application in the list.
      b. Click the **Delete** button.

10. Click **OK** to save the changes and close the **Rule properties** window.

    The new exclusion is created and displayed in the list of exclusions.

c. If you need to modify an exclusion, click the **Modify** button.

d. If you need to delete an exclusion, select the exclusion and click the **Delete** button.

5. If you are configuring the policy settings, make sure that the switch in the upper right corner of the group of settings is turned on. It is the default position of the switch.

6. Click **OK** to save the changes.

Configuring storage settings in Kaspersky Endpoint Agent

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section describes how to configure the quarantine settings and data synchronization settings with the Administration Server by means of Kaspersky Endpoint Agent Management plug-in.

About Kaspersky Endpoint Agent quarantine

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Quarantine is a special local repository on the device. The user can put files considered dangerous to the computer into quarantine. 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 Network Agent 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can use Kaspersky Security Center to configure quarantine settings, view the properties of the quarantined objects on the protected devices, 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 documentation.

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.

Kaspersky Endpoint Agent quarantines object under the system account (SYSTEM).

Quarantined objects can be removed using 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure 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. For example, if Kaspersky Endpoint Agent is installed on drive C, the path to the Quarantine folder will be 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 will publish the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but will 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 will publish the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but will 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. For example, if Kaspersky Endpoint Agent is installed on drive C, the path to the folder with the objects restored from quarantine will be C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored.

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

8. Click the **Apply** button and then click **OK**.

The quarantine settings and the folder for restoring objects from quarantine have been configured.

Configuring data synchronization with the Administration Server

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure synchronization of data on quarantined objects on managed devices with Kaspersky Security Center Administration Server. Data synchronization is required to manage quarantine using Kaspersky Security Center.

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 the Administration Server** subsection, select the **Data about objects, quarantined on managed devices** check box.
6. In the upper right corner of the settings group, change the switch from **Unaffected by policy** to **Under policy**.
7. Click the **Apply** button and then click **OK**.

Data synchronization with the Administration Server is configured.

Configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Before performing the following steps, get the MDR configuration file. It contains a configuration file (BLOB) required for integration.

If you want Kaspersky Endpoint Agent to process data about events generated by Kaspersky Industrial CyberSecurity for Networks and send this data to Kaspersky Managed Detection and Response, configure interaction with Kaspersky Security Center in the settings of Kaspersky Industrial CyberSecurity for Networks. For detailed information on configuring interaction between the applications, refer to the *Kaspersky Industrial CyberSecurity for Networks Help*.

Integration with Kaspersky Managed Detection and Response is only available for Kaspersky Endpoint Agent Management plug-in versions 3.9.2 and later.

In order to configure integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response using the Kaspersky Security Center Administration Console:

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 **Managed Detection and Response** section.
5. In the **Managed Detection and Response settings** group, do the following:
   a. Select the **Enable Managed Detection and Response** check box.
   b. Click the **Upload configuration file (BLOB)** button and select the BLOB configuration file to load.

      By downloading the Managed Detection and Response configuration file, you agree to automatically send the specified data from the device with Kaspersky Endpoint Agent installed to Kaspersky for processing. Do not download the configuration file if you do not want the specified information to be processed.

   c. In the **User identifier** field, enter an arbitrary value.
6. In the policy properties window, click **OK**.

Integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response is configured.

MDR operation when using Kaspersky Endpoint Agent simultaneously with Kaspersky Endpoint Security

Kaspersky Endpoint Security 11 or later with the current database version supports interaction with MDR. In Kaspersky Endpoint Security 11.6.0 or later, interaction with MDR is available immediately after installation.

If you use Kaspersky Endpoint Agent to work with MDR and install Kaspersky Endpoint Security of the version that supports interaction with MDR or update Kaspersky Endpoint Security 11 or later databases to the current version, MDR stops working with Kaspersky Endpoint Agent and becomes available for work with Kaspersky Endpoint Security. At that:

- Switching between Kaspersky Endpoint Agent and Kaspersky Endpoint Security is performed in quiet mode.
- Kaspersky Endpoint Agent allows for configuring settings for interaction with MDR, but these settings are not applied on the device.

- If Kaspersky Endpoint Security is not available (for example, you uninstalled the application), MDR can start working with Kaspersky Endpoint Agent if you restart the Kaspersky Endpoint Agent service.
- The Managed Detection and Response component remains in the *Running* status in Kaspersky Endpoint Agent settings on the device, since Kaspersky Endpoint Agent continues to communicate with MDR (for example, to resume working with the solution if necessary).

Configuring failure diagnosis

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent does not automatically create a folder for storing trace or dump files on the device. Specify a folder that is already available on the device.

To configure failure diagnosis:

1. **Open the application properties window for an individual device**.
    1. 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.
    2. In the workspace, select the **Devices** tab.
    3. Select the device for which you want to configure Kaspersky Endpoint Agent settings.
    4. Select **Properties** in the device context menu.

       The device properties window opens.
    5. Select the **Applications** section.

       A list of Kaspersky applications installed on the device is displayed in the window.
    6. 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 **Application settings** section select the **Failure diagnosis** subsection.

3. To enable logging of debug information to the trace files:

    a. Enable the **Write debug information to trace files** option.

    b. In the **Trace files folder** field, specify the path to the folder on the device where the application saves the trace files.

    > Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

    c. In the **Maximum trace file size (MB)** field, specify the file size in megabytes.

    The default value is 50 MB. When the specified file size is reached, the application continues writing to a new file.

4. If you want the application to overwrite old trace files:

    a. Enable the **Overwrite old trace files** option.

    b. Enter the desired value in the **Maximum number of files per trace log** field.

    The default value is 1 file. When the specified number of files is reached, the application overwrites old files, starting with the oldest one. The specified limit is applied separately for each Kaspersky Endpoint Agent process being debugged, so the total number of files for all processes may exceed the specified value.

5. To enable logging of dump files:

    a. Enable the **Create dump files** option.

    b. In the **Dump files folder** field, specify the folder to save the dump files.

    > Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

6. Click **OK**.

Failure diagnostics is configured and enabled for all Kaspersky Endpoint Agent processes that are currently running. Failure diagnostics files will be generated in the folders you specified.

Managing Kaspersky Endpoint Agent tasks

This section describes how to manage Kaspersky Endpoint Agent tasks.

Creating a local task

Local tasks are run on a specific device. For more information on tasks, refer to Kaspersky Security Center documentation.

To create a local task:

1. Open Kaspersky Security Center Administration Console.
2. In the 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 that includes the desired 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 will start.
7. Select the required task and click **Next**.
8. Follow the instructions of the task creation wizard.

Creating a group task

Group tasks are performed on the devices of the selected administration group. For more information on tasks, refer to Kaspersky Security Center documentation.

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 will start.
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 tasks appears.

Deleting a task from the list

To remove tasks from 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.
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 the actions you can perform on the tasks will be displayed.
4. Select the **Delete** action.
   The action confirmation window opens.
5. Click **Yes**.

The selected tasks will be deleted from the list.

Starting tasks manually

You can start the created tasks manually. For example, you can manually start the tasks for which scheduled start is not configured.

To start a task manually:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.
   A list of tasks appears.
3. In the context menu of the desired task, select the **Run** action.

The task will run.

Starting tasks by schedule

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the scheduled task start:

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 **Time** and **Date** lists, select the date and time from which the schedule applies.
5. To configure advanced schedule settings, click the **Advanced** button and configure the following settings in the **Advanced** window:
   - **Quit tasks, running longer than**

     Enable this setting if you want to set a task execution time limit. After the specified time, the task will automatically terminate.
   - **Cancel schedule from**

     Enable this setting if you want to specify a schedule expiration date. After the specified date, the schedule will expire.
   - **Run missed tasks**

     Enable this option if you want the application to start tasks that were not completed on time as soon as possible.
   - **Randomize the task run to every**

     Enable this option if you want to avoid a scenario where a large number of workstations simultaneously access the Administration Server by running the task on each workstation at a random moment within the specified time interval.
6. Click **OK**.

Scheduled task start has now been configured and applied on devices.

Viewing task execution results

You can view the task execution results during their storage period. You can also 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 result:

1. Open Kaspersky Security Center Administration Console.
2. In Kaspersky Security Center Administration Console tree, open the **Tasks** folder.

   A list of tasks 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 will open.

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 change the 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 tasks 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 the task execution results to be stored.
7. Click the **Apply** button and then click **OK**.

It is not recommended to shorten the storage period for IOC Scan task execution results.

Creating Kaspersky Endpoint Agent activation task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 **Application activation** task creation wizard for the desired scope in one of the following ways:

   - Start the local task creation wizard.
   - **Start the group task creation wizard**.

     Group tasks are performed on the devices of the selected administration group. For more information on tasks, refer to Kaspersky Security Center documentation.

     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 will start.

     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 documentation.

4. If you want to add this license key as an additional one to automatically renew the license, select the **Use as additional key** 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 documentation.

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 documentation.

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 for the selected device or device group has been created.

Managing Kaspersky Endpoint Agent database and module update tasks

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section provides instructions on how to create and configure the Database and application module update task.

Creating Database and application module update task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 will start.
4. Select the **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 will start.

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 **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 the **Update servers** button.

      2. In the new line, enter the address of the update server (HTTP or FTP), or the path to the network or local folder containing the update files.

      3. If you want to use this server to update databases, select the check box next to its address. You can also add servers to the list and clear the check boxes next to the addresses of the 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.

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 updates**. Kaspersky Endpoint Agent will not check the availability of application module updates.
      - **Only check for availability of critical software modules updates**. Kaspersky Endpoint Agent will check the availability only for important application module updates.
      - **Download and install critical application module updates**. 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 application module updates** check box.

3. **Configuring the 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 **Time** and **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 **Stop tasks that run 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 as well as to run the task on workstations not precisely 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**.

4. **Selecting the devices on which the task will be performed**

   In the device selection window that opens, select the devices for which you want to assign the task and click **Next**.

   For example, you can select the **Assign task for an administration group** option and select an administration group from the list.

5. **Selecting the Kaspersky Security Center user account 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

After creating the Database and application module update task, you can configure the settings for this task.

To modify 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 tasks 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:

- **Task name**

  Do the following:

  1. Select the **General** section.
  2. Change the task name in the top line.

- **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 will open 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 the 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 with managed devices, refer to the *Kaspersky Security Center Help*.

- **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 the **Update servers** button.
        2. In the new line, enter the address of the update server (HTTP or FTP), or the path to the network or local folder containing the update files.
        3. If you want to use this server to update databases, select the check box next to its address. You can also add servers to the list and clear the check boxes next to the addresses of the 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.

- **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 updates**. Kaspersky Endpoint Agent will not check the availability of application module updates.
     - **Only check for availability of critical software modules updates**. Kaspersky Endpoint Agent will check the availability only for important application module updates.
     - **Download and install critical application module updates**. 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 application module updates** check box.

- **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 **Time** and **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 **Stop tasks that run 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 as well as to run the task on workstations not precisely 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 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.

- **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 provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

When 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 the following types of IOC Scan tasks:

- *Standard IOC Scan tasks* are group or local tasks that are created and configured manually in Kaspersky Security Center or through the command line interface. IOC files prepared by the user are used to run the tasks.

- *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, as well as infected and probably infected objects in the event and detection database, and also to scan computers on which Kaspersky Endpoint Agent is installed.

Different tasks are managed in different ways and have different configurable settings and task scopes. A 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 using the command line interface, without integration with third-party systems. IOC files prepared by the user are used to run the tasks. The task settings do not depend on the policy settings. The **Retrospective IOC scan** mode is available for tasks. You can specify the following actions as responses to detected IOCs (not available when running the tasks from the command line): • Run on-demand scan tasks using EPP on the device. • Enable network isolation of the device. Viewing reports is available both in the task execution results as a summary table and in the Detected IOC card.	Local or 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 the IOC scan schedule for computers with Kaspersky Endpoint Agent in the web interface of Kaspersky Anti Targeted Attack Platform. Task management using Kaspersky Security Center or using the command line is not supported. No actions are automatically performed when an IOC is detected. 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 for 7 days after the task is executed, or until the task is removed.

Managing IOC Scan tasks in Kaspersky Endpoint Agent

You can manage IOC Scan tasks using Kaspersky Security Center or using the Kaspersky Endpoint Agent command line interface, and you can also download IOC files and configure the IOC scan schedule in the 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. • Viewing detailed reports on the task execution results as a summary table and in the Detected IOCs card. • IOC collection export. • Configuring the following task settings in the task creation wizard or in the task properties after the task creation: • IOC collection settings. • IOC scan settings. • Application actions upon IOC detection (network isolation of the device and start of the scan tasks using EPP on the device). • Task schedule settings. • 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. • Viewing data on the task's execution.
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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Standard IOC Scan tasks are group or local tasks that are created and configured manually in Kaspersky Security Center or through the command line interface. IOC files prepared by the user are used to run the tasks.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

This section provides instructions on how to manage Standard IOC Scan tasks.

Requirements for IOC files

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

When creating IOC Scan tasks, consider the following requirements and limitations related to 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.
- Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.
- 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.
- The size of a single IOC file must not exceed 3 MB. Using larger files results in the failure of IOC Scan tasks. In this case, the total size of all added files in the IOC collection can exceed 3 MB.
- It is recommended to create one IOC file per each threat. This makes it easier to read the results of the IOC Scan task.

The table below shows the features and limitations of the OpenIOC standard supported by the application.

Features and limitations of the OpenIOC standard versions 1.0 and 1.1

Supported conditions	OpenIOC 1.0:
	
	`is`
	`isnot` (as an exclusion from the set)
	`contains`
	`containsnot` (as an exclusion from the set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Supported condition attributes	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Supported operators	`AND` `OR`
Supported data types	`date`: date (applicable conditions: `is`, `greater-than`, `less-than`) `int`: integer number (applicable conditions: `is`, `greater-than`, `less-than`) `string`: string (applicable conditions: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `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`.
	
	The application supports interpretation of the `Content` parameter specified as intervals for the following data types: `int` and `date`:
	
	OpenIOC 1.0:
	Using the `TO` operator in the `Content` field:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Using the `greater-than` and `less-than` conditions
	Using the `TO` operator in the `Content` field
	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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the 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.
- **Start the group task creation wizard**.

  Group tasks are performed on the devices of the selected administration group. For more information on tasks, refer to Kaspersky Security Center documentation.

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 will start.
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 **Select folder** item to add a group of IOC files to the IOC collection.
     - Select the **Select 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 to get information about each IOC file, click **View**.

     The **Select 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 **Select 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 select data types (IOC documents) that you want to analyze during IOC scan and configure the additional scan settings:

  1. Click the **Configure IOC terms and documents** button.

     The **IOC terms and documents** window opens.

  2. In the **Select data types (IOC documents) to analyze during IOC scanning** group of settings, select the check boxes next to the required IOC documents.

     Depending on the loaded IOC files, some check boxes may be disabled.

     Kaspersky Endpoint Agent automatically selects data types (IOC documents) for the IOC Scan task in accordance to the contents of the downloaded IOC files. It is not recommended to unselect data types manually.

  3. To configure additional settings for the selected ProcessItem IOC document:

     a. Click the **Advanced (ProcessItem)** button.

        The **ProcessItem document scan settings** window opens.

     b. In the **Indicators** group of settings, select data that you want to analyze during the task execution.

     c. Click **OK** to save the changes and close the **ProcessItem document scan settings** window.

  4. To configure additional settings for the selected FileItem IOC document:

     a. Click the **Advanced (FileItem)** button.

        The **FileItem document scan settings** window opens.

     b. On the **Scan areas** tab, select data that you want to analyze during the task execution.

     c. On the **Scan areas** tab, select the areas on protected device drives where to look for indicators of compromise.

        You can select one of the predefined areas, or specify the paths to the desired areas manually.

     d. On the **Exclusions** tab, select the **Apply exclusions** check box and specify the paths to the areas on the protected device drives that do not need to be scanned during the task execution.

     e. Click **OK** to save the changes and close the **FileItem document scan settings** window.

  5. To configure additional settings for the selected RegistryItem IOC document:

     a. Click the **Advanced (RegistryItem)** button.

        The **RegistryItem document scan settings** window opens.

b. Specify the Windows registry keys to be scanned during the task execution.

You can select to scan predefined registry keys or specify the list of required registry keys manually.

c. Click **OK** to save the changes and close the **RegistryItem document scan settings** window.

6. To configure additional settings for the selected EventLogItem IOC document:

a. Click the **Advanced (EventLogItem)** button.

The **EventLogItem document scan settings** window opens.

b. To ignore the events that were logged before the specified moment, select the **Scan only events logged during the specified period** check box and specify date and time.

c. If necessary, in the bottom of the window, edit the predefined list of channels that are analyzed during the task execution.

d. Click **OK** to save the changes and close the **EventLogItem document scan settings** window.

7. Click **OK** to save the changes and close the window.

The saved settings will be applied when the task is executed.

- **Retrospective IOC scan**

Retrospective IOC scan is an operation mode of the IOC Scan task, when Kaspersky Endpoint Agent searches for indicators of compromise based on the data received during a time interval specified by the user. This mode is intended for searching for indicators of compromise based on the data on network activity of protected devices. Kaspersky Endpoint Agent analyzes data in the operating system logs and in browsers on devices.

The **Retrospective IOC scan** mode is available only for Standard IOC Scan tasks.

To enable the Retrospective IOC scan mode:

1. In the **Retrospective IOC Scan** group of settings enable the **Perform Retrospective IOC Scan within the interval** option.

2. Specify the time interval.

During the task execution, the application analyzes data collected during the specified time interval, including the boundaries of the specified interval (from 00:00 on the start date until 23:59 on the end date). The default interval starts at 00:00 on the day preceding the task creation day and ends at 23:59 on the day when the task was created.

If during execution of the IOC Scan task with the **Perform Retrospective IOC Scan within the interval** option enabled the application does not find any data for the specified time interval to be analyzed, it does not inform about this. In this case, the application shows no indicators of compromise in the task completion report.

- **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 indicator of compromise is found** 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 **Run critical areas scan on the device** 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.

  When configuring the task settings in Kaspersky Security Center Administration Console, the **Do not perform actions on critical system files** check box is available only if the **Quarantine and delete** response action is selected for the task (this setting can be configured only in Kaspersky Security Center Web Console).

- **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 **Time** and **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 **Stop tasks that run 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 as well as to run the task on workstations not precisely 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**.

- **Running the task from a Kaspersky Security Center user account**

  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 an 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

To configure the Standard IOC Scan task settings:

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 will open.

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 changes and click **Apply**, and then click **OK**.

   Configuration of the Standard IOC Scan task settings is now finished.

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 **Select folder** item to add a group of IOC files to the IOC collection.
     - Select the **Select 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 to get information about each IOC file, click **View**.

   The **Select 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 **Select 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.

- **Retrospective IOC scan**

  Retrospective IOC scan is an operation mode of the IOC Scan task, when Kaspersky Endpoint Agent searches for indicators of compromise based on the data received during a time interval specified by the user. This mode is intended for searching for indicators of compromise based on the data on network activity of protected devices. Kaspersky Endpoint Agent analyzes data in the operating system logs and in browsers on devices.

  The **Retrospective IOC scan** mode is available only for Standard IOC Scan tasks.

  To enable the Retrospective IOC scan mode:

  1. In the **Retrospective IOC Scan** group of settings enable the **Perform Retrospective IOC Scan within the interval** option.

  2. Specify the time interval.

     During the task execution, the application analyzes data collected during the specified time interval, including the boundaries of the specified interval (from 00:00 on the start date until 23:59 on the end date). The default interval starts at 00:00 on the day preceding the task creation day and ends at 23:59 on the day when the task was created.

  If during execution of the IOC Scan task with the **Perform Retrospective IOC Scan within the interval** option enabled the application does not find any data for the specified time interval to be analyzed, it does not inform about this. In this case, the application shows no indicators of compromise in the task completion report.

- **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 indicator of compromise is found** 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 **Run critical areas scan on the device** 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.

  When configuring the task settings in Kaspersky Security Center Administration Console, the **Do not perform actions on critical system files** check box is available only if the **Quarantine and delete** response action is selected for the task (this setting can be configured only in Kaspersky Security Center Web Console).

- **Data types (IOC documents) to be analyzed during IOC scan**

  To select data types (IOC documents) that you want to analyze during IOC scan and configure the additional scan settings:

  1. Open the **Advanced** section.
  2. In the **Select data types (IOC documents) to analyze during IOC scanning** group of settings, select the check boxes next to the required IOC documents.

     Depending on the loaded IOC files, some check boxes may be disabled.

     Kaspersky Endpoint Agent automatically selects data types (IOC documents) for the IOC Scan task in accordance to the contents of the downloaded IOC files. It is not recommended to unselect data types manually.

  3. To configure additional settings for the selected ProcessItem IOC document:

     a. Click the **Advanced (ProcessItem)** button.

     The **ProcessItem document scan settings** window opens.

     b. In the **Indicators** group of settings, select data that you want to analyze during the task execution.

     c. Click **OK** to save the changes and close the **ProcessItem document scan settings** window.

  4. To configure additional settings for the selected FileItem IOC document:

     a. Click the **Advanced (FileItem)** button.

     The **FileItem document scan settings** window opens.

     b. On the **Scan areas** tab, select data that you want to analyze during the task execution.

c. On the **Scan areas** tab, select the areas on protected device drives where to look for indicators of compromise.

You can select one of the predefined areas, or specify the paths to the desired areas manually.

d. On the **Exclusions** tab, select the **Apply exclusions** check box and specify the paths to the areas on the protected device drives that do not need to be scanned during the task execution.

e. Click **OK** to save the changes and close the **FileItem document scan settings** window.

5. To configure additional settings for the selected RegistryItem IOC document:

a. Click the **Advanced (RegistryItem)** button.

The **RegistryItem document scan settings** window opens.

b. Specify the Windows registry keys to be scanned during the task execution.

You can select to scan predefined registry keys or specify the list of required registry keys manually.

c. Click **OK** to save the changes and close the **RegistryItem document scan settings** window.

6. To configure additional settings for the selected EventLogItem IOC document:

a. Click the **Advanced (EventLogItem)** button.

The **EventLogItem document scan settings** window opens.

b. To ignore the events that were logged before the specified moment, select the **Scan only events logged during the specified period** check box and specify date and time.

c. If necessary, in the bottom of the window, edit the predefined list of channels that are analyzed during the task execution.

d. Click **OK** to save the changes and close the **EventLogItem document scan settings** window.

7. Click **OK** to save the changes and close the window.

The saved settings will be applied when the task is executed.

- **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 **Time** and **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 **Stop tasks that run 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 as well as to run the task on workstations not precisely 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 an 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 devices 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 tasks 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 card** button.

   Detected IOC 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 IOC card is not available for IOC files, for which no indicators of compromise were detected during scan.

Managing Kaspersky Endpoint Agent using Kaspersky Security Center Web Console

You can centrally manage several protected devices with Kaspersky Endpoint Agent installed, that are included in the administration group, by means of Kaspersky Endpoint Agent Management web plug-in. Kaspersky Security Center Web Console also lets you separately configure the operation settings of each protected device in the administration group.

An administration group is created manually in Kaspersky Security Center Web Console and includes several devices with Kaspersky Endpoint Agent installed, for which the same control and protection settings can be configured. For details on using administration groups, see Kaspersky Security Center Help.

Application settings for an individual protected device cannot be configured if Kaspersky Endpoint Agent operation on this protected device is controlled by an active Kaspersky Security Center policy.

Kaspersky Endpoint Agent can be managed from Kaspersky Security Center Web Console in the following ways:

- Using Kaspersky Security Center policies. Kaspersky Security Center policies can be used to remotely configure the same protection settings for a group of devices. Task settings specified in the active policy have priority over task settings configured locally in the Application Console or remotely in the device properties window of Kaspersky Security Center Web Console.
- You can use policies to configure general application settings, Real-Time Protection task settings, Local Activity Control tasks settings, and scheduled system task start settings.
- Using Kaspersky Security Center group tasks. Kaspersky Security Center group tasks allow remote configuration of common settings of tasks with a limited execution period for a group of devices.
- You can use group tasks to activate the application, configure On-Demand Scan task settings, update task settings, and Rule Generator for Applications Launch Control task settings.
- Using tasks for a set of devices. Tasks for a set of devices allow remote configuration of common settings of tasks with a limited execution period for protected devices that do not belong to any administration group.
- Using the properties window of a single device. In the device properties window, you can remotely configure the task settings for a single protected device included in the administration group. You can configure both general application settings and the settings of all Kaspersky Endpoint Agent tasks if the selected protected device is not controlled by an active Kaspersky Security Center policy.

Kaspersky Security Center Web Console makes it possible to configure application settings and advanced features, and lets you work with logs and notifications. You can configure these settings for a group of protected devices as well as for an individual protected device.

Google Chrome for Windows is required to manage Kaspersky Endpoint Agent using Kaspersky Security Center Web Console.

Managing Kaspersky Endpoint Agent policies

This section describes how to create Kaspersky Endpoint Agent policies and enable policy settings.

Creating Kaspersky Endpoint Agent policy

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To create a Kaspersky Endpoint Agent policy in the Kaspersky Security Center Web Console:

1. In the main window, select **Devices** → **Policies and profiles**.
2. Click the **Add** button.

   The policy creation wizard starts.
3. Select the Kaspersky Endpoint Agent application and click **Next**.
4. Select the required Kaspersky Endpoint Agent deployment method by selecting the appropriate check boxes:
   - **Integration with Kaspersky Sandbox**
   - **Endpoint Detection and Response Optimum**
   - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks.**

   Policy type and integration with Kaspersky Sandbox and KATA EDR cannot be selected in Kaspersky Security Center Cloud Console.
5. Click **Next**.
6. On the **General** tab, you can perform the following actions:
   - Change the policy name.
   - Select policy status:
     - **Active**. After the next synchronization, the policy will be active on the computer.
     - **Inactive**. Backup policy. An inactive policy can be made active, if required.
     - **Out-of-office**. The policy will become active when the computer leaves the corporate network.

- Configure the policy settings inheritance:
  - **Inherit settings from parent policy**. If this option is enabled, the policy settings will be inherited from the upper-level policy. The policy settings cannot be modified if the **Force inheritance of settings in child policies** option is enabled in the parent policy.
  - **Force inheritance of settings in child policies**. If this option is enabled, the parent policy settings will be applied to child policies. In the properties window of the child policy, the **Inherit settings from parent policy** option is automatically enabled and cannot be disabled.

7. On the **Application settings** tab, you can configure Kaspersky Endpoint Agent policy settings.
8. Click the **Save** button.

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 the policy properties window**.
   1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
   2. Select the policy you want to configure.
   3. In the **<Policy name>** window that opens, select the **Application settings** tab.
2. Select the section and group of settings to which the required setting belongs.
3. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   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.

Opening Kaspersky Endpoint Agent settings window

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To open the Kaspersky Endpoint Agent policy settings window:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.

To open the Kaspersky Endpoint Agent settings window for an individual device:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
2. Select the device.
3. In the **<Device name>** window that opens, select the **Applications** tab.
4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

If an active Kaspersky Security Center policy is applied to a device and blocks changes to the application settings, these settings cannot be edited in the **Application settings** window, except for the network isolation settings.

The settings of automatic network isolation can be configured in the policy properties, and the settings of network isolation on demand (manually enabled settings) can be configured in the properties of an individual device.

Configuring Kaspersky Endpoint Agent security settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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.
- Password protect actions in the application.
- Enable the application self-defense mechanism.

Configuring user permissions

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. Do one of the following:
   - **Open the application properties window for an individual device**.
     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.
   - **Open the policy properties window**.
     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.
2. In the **Application settings** section select the **Security settings** subsection.
3. In the **User permissions for application service management** group of settings, click the **Configure** button next to the name of the required setting (**User permissions for application management** or **Configure user permissions for application management**).

   To add users and user groups, specify the security descriptor strings using the Security Descriptor Description Language (SDDL).
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.

5. Click **OK**.

6. Click the **Save** button.

Enabling Password protection

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Unrestricted user access to the application and its settings can reduce the security level of the device. Password protection is a means to limit user access to the application.

To enable password protection:

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - **Open the policy properties window**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.

3. In the **Password protection** group of settings select the **Apply password protection** check box.

4. Enter a password and confirm it.
   It is recommended to select a password that meets the following requirements:

   - The password must be at least 8 characters long.
   - The password must not contain the user's account name.
   - The password must not match the name of the device on which Kaspersky Endpoint Agent is installed.

- The password must contain characters from at least three of the following groups:
  - uppercase characters (A-Z);
  - lowercase characters (a-z);
  - numbers (0-9);
  - special characters (!$#%).

5. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
6. Click **OK**.
7. Click the **Save** button.

Password protection is now enabled. If a user attempts to perform a password protected action, the application will prompt 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 login attempts after many attempts of entering an incorrect password.

Enabling and disabling Self-Defense

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The *Self-Defense mechanism* of Kaspersky Endpoint Agent provides protection from malware that tries to lock or delete the application. The Self-Defense mechanism prevents the 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. Do one of the following:
   - **Open the application properties window for an individual device**.
     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.

4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

- **Open the policy properties window**.
  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. In the **Self-defense** group of settings, enable or disable the **Enable self-defense for application modules in memory** setting.
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. Click the **Save** button.

The Self-Defense mechanism is now enabled or disabled.

Configuring Kaspersky Endpoint Agent connection settings to a proxy server

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Proxy server connection settings are used for updating databases, activating the application, and external services.

If you want to **Use proxy server with the specified settings** when connecting to KATA, Kaspersky Industrial CyberSecurity for Networks or Kaspersky Sandbox server, make sure that the **Connect using the proxy server if specified in the general settings** option is selected when configuring integration with KATA, Kaspersky Industrial CyberSecurity for Networks or Kaspersky Sandbox. This option is not selected by default.

To configure proxy server connection settings:

1. Do one of the following:

- **Open the application properties window for an individual device**.
  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
  2. Select the device.

3. In the **<Device name>** window that opens, select the **Applications** tab.
4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

- **Open the policy properties window**.
  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. Select one of the following proxy service usage options:
   - **Do not use proxy server**.
   - **Automatically detect proxy server address**.
   - **Use proxy server with specified settings**.
4. If you select the **Automatically detect proxy server address** option, the proxy server for further telemetry transmission will be detected automatically.
5. 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.
6. If you want to use NTLM authentication to connect 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.
7. 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.
8. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
9. Click **OK**.
10. In the policy properties window, click **Save**.

Proxy server connection settings are now configured.

Configuring Kaspersky Security Center as a proxy server for Kaspersky Endpoint Agent activation

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To enable usage of Kaspersky Security Center as a proxy server for the application activation:

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - **Open the policy properties window**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Application settings** section select the **Security settings** subsection.
3. In the **Licensing** group of settings, select the **Use Kaspersky Security Center as a proxy server when activating the application** check box.
4. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.
5. Click **OK**.
6. In the policy properties window, click **Save**.

Kaspersky Security Center usage as a proxy server for Kaspersky Endpoint Agent activation is now enabled.

Configuring Kaspersky Endpoint Agent policy type

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Selecting Kaspersky Endpoint Agent's policy type is necessary in order for the list of settings displayed in the policy to correspond to the selected Kaspersky Endpoint Agent deployment method.

To configure the policy type:

1. **Open the policy properties window**.
    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
    2. Select the policy you want to configure.
    3. In the **<Policy name>** window that opens, select the **Application settings** tab.
2. In the **Application settings** section select the **Management and interface** subsection.
3. In the window that opens, select the required Kaspersky Endpoint Agent deployment method by selecting the appropriate check boxes:
    - **Integration with Kaspersky Sandbox**
    - **Endpoint Detection and Response Optimum**
    - **Endpoint Detection and Response Expert (KATA EDR), Kaspersky Industrial CyberSecurity for Networks**

    Policy type and integration with Kaspersky Sandbox and KATA EDR cannot be selected in Kaspersky Security Center Cloud Console.
4. Click **OK**.

The policy type has been changed. The policy contains the settings for the selected Kaspersky Endpoint Agent deployment method.

Configuring KSN usage in Kaspersky Endpoint Agent

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To protect your computer more effectively, Kaspersky Endpoint Security uses data received from users around the globe. Kaspersky Security Network is designed to receive this data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services that provide access to the online Kaspersky Knowledge Base that contains information about the reputations of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by the EPP application 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 parts of files, that may be exploited by intruders to harm the computer or data can be also sent to Kaspersky to be further examined.

No personal data is collected, processed, or stored. The types of data that Kaspersky Endpoint Agent sends to Kaspersky Security Network are described in the KSN Statement.

Participation in Kaspersky Security Network is voluntary. KSN usage is disabled by default. After enabling KSN usage, you can disable this option at any time.

Starting from version 3.10, Kaspersky Managed Protection (also referred to as KMP) usage cannot be configured by means of Kaspersky Endpoint Agent. If usage of the KMP service was enabled in the previous Kaspersky Endpoint Agent version, the KMP service continues functioning after the application is updated to version 3.10 and later. After the application update, you can disable the KMP service only using Kaspersky Endpoint Agent Administration Plug-in or Kaspersky Endpoint Agent Web Plug-in of versions earlier then 3.10.

To enable KSN usage:

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - **Open the policy properties window**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Kaspersky Security Network** section, click the **Read terms and conditions of the KSN Statement** link and perform the following actions:

   a. In the right part of the window, review the terms and conditions of the KSN Statement.

   b. If you agree with terms and conditions of the Statement, select the **I confirm that I have fully read, understood, and accept the terms and conditions of this Kaspersky Security Network Statement** check box.

   c. Click **OK**.

3. Select the **Enable Kaspersky Security Network usage** check box.

4. If you want to use Kaspersky Security Center for telemetry transmission, select the **Use Kaspersky Security Center as a KSN proxy server** check box.

5. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.

6. Click **OK**.

7. In the policy properties window, click **Save**.

KSN usage is enabled.

Configuring integration between Kaspersky Endpoint Agent and KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure integration between Kaspersky Endpoint Agent and the KATA Central Node component using the Kaspersky Security Center Web Console.

Configuring data submission settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure data submission settings:

1. **Open the policy properties window**.
    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
    2. Select the policy you want to configure.
    3. In the **<Policy name>** window that opens, select the **Application settings** tab.
2. In the **Telemetry collection servers** section, select the **General settings** subsection.
   The **General settings** window opens.
3. In the **Data submission settings** group, do the following:
    - Specify the value in the **Events transmission period (sec.)** field.
    - Specify the value in the **Maximum number of events in a package** field.
4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.
   The default switch position is **Enforce**.
5. Click **OK**.

Configuring request throttling settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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 the policy properties window**.
    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
    2. Select the policy you want to configure.
    3. In the **<Policy name>** window that opens, select the **Application settings** tab.
2. In the **Telemetry collection servers** section, select the **General settings** subsection.
   The **General settings** window opens.
3. In the **Request throttling** group of settings, you can perform the following actions:
    - Select or clear the **Enable request throttling** check box to enable or disable the feature.
      This feature is enabled by default.

- Specify the value in the **Maximum number of 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 **Percentage of event limit excess** 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. You can specify a value from 5% to 100%. The default value is 15%.

4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

5. Click **OK**.

Enabling and disabling integration with KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you use Nginx as a proxy server between a device with Kaspersky Endpoint Agent installed and KATA 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 KATA for processing. Otherwise, Nginx will not send objects whose size exceeds the specified value. The default value is 1 MB.

To enable or disable integration with the KATA Central Node component:

1. **Open the policy properties window**.

   1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.

   2. Select the policy you want to configure.

   3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Telemetry collection servers** section, select the **Integration with KATA** subsection.

   The **KATA integration** window opens.

3. In the **Connection settings** group, do one of the following:

   - To enable integration with KATA Central Node:

     a. Select the **Enable KATA integration** check box.

     b. In the **List of KATA servers** settings group, for one or more KATA servers, specify the IP address or full domain name of the KATA server, as well as the port for connecting to the server.

     Kaspersky Endpoint Agent connects to the first server in the list. If the connection does not succeed, Kaspersky Endpoint Agent connects to the second server and so on down the list.

   - To disable integration with KATA Central Node, clear the **Enable KATA integration** check box.

4. Enable or disable the **Connect using the proxy server if specified in the general settings** option.

   This option is disabled by default. The application connects to the KATA server only directly and does not use the general proxy server connection settings. You can enable this option if you want the application to use the general proxy server connection settings when connecting to the KATA server.

5. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

6. Click **OK**.

Integration with KATA Central Node is enabled or disabled.

Configuring trusted connection with KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure trusted connection between Kaspersky Endpoint Agent and KATA Central Node, perform the following actions on Kaspersky Endpoint Agent side:

1. **Open the policy properties window**.

   1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.

   2. Select the policy you want to configure.

   3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Telemetry collection servers** section, select the **Integration with KATA** subsection.

   The **KATA integration** window opens.

3. In the **Connection settings** group, select the **Use pinned certificate to protect connection** check box.

4. Click the **Add new TLS certificate** button.

   The window for adding a new TLS certificate opens.

5. Perform one of the following actions to add a TLS certificate:

   - Add a certificate file. Click **Upload**, and in the window that opens, select the certificate file and click **Open**.
   - Copy and paste the contents of the certificate file to the **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.

6. Click **OK**.

   Information about the added TLS certificate is shown in the **TLS certificate data** group of settings.

7. If you want to configure additional connection protection by a user certificate, do the following:

   a. Select the **Secure connection with the client certificate** check box.

   b. Click the **Load Crypto-container** button.

   c. In the window that opens select the PFX archive and click **Open**.

   d. In the **Crypto-container password** field, enter the password for the PFX archive.

   e. Click **OK**.

8. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.

9. Click **OK**.

A Trusted connection to the KATA server is now configured.

The TLS certificate file 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 or DER format.
- The private key length must be 2048 bits or longer.

For more details about preparing TLS certificates for import, refer to OpenSSL documentation.

Configuring synchronization settings between Kaspersky Endpoint Agent and KATA Central Node

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure synchronization settings between Kaspersky Endpoint Agent and KATA Central Node:

1. **Open the policy properties window**.
    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
    2. Select the policy you want to configure.
    3. In the **<Policy name>** window that opens, select the **Application settings** tab.
2. In the **Telemetry collection servers** section, select the **Integration with KATA** subsection.

   The **KATA integration** window opens.
3. In the **Additional settings** group, configure the following settings:
    - **Timeout (sec.)**. Specify the maximum KATA server response timeout. The default value is 10 seconds.
    - **Send synchronization 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. The default value is 5 minutes.
    - Select or clear the **Use TTL period when sending events** check box. The check box is cleared by default.

      If the check box is selected, Kaspersky Endpoint Agent does not send information about the processes that are started again to the KATA server. Kaspersky Endpoint Agent does not consider the launch of the process as repeated if the process is started after the end of the TTL period.
    - If you select the **Use TTL period when sending events** check box, specify the time in the **TTL period (min.)** field. The default value is 1440 minutes.
4. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

   The default switch position is **Enforce**.
5. Click **OK**.

Configuring EDR telemetry settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section contains information on how to configure:

- Exclusions for EDR telemetry about application processes, which Kaspersky Endpoint Agent processes and sends to a server with the KATA Central Node or Kaspersky Industrial CyberSecurity for Networks component.
- Optimization of the volume of EDR telemetry that Kaspersky Endpoint Agent processes and sends to a server with the Kaspersky Industrial CyberSecurity for Networks component.
- Exclusions for EDR telemetry about network communications, which Kaspersky Endpoint Agent processes and sends to a server with the Kaspersky Industrial CyberSecurity for Networks component.

Enabling and configuring exclusions for and optimization of sent EDR telemetry about application processes

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can enable and configure exclusions for and optimization of EDR telemetry about application processes using Kaspersky Security Center Web Console, in the properties of an individual device or in the policy settings for a group of devices.

Exclusions for EDR telemetry about application processes are available when Kaspersky Endpoint Agent is integrated with servers where KATA Central Node or Kaspersky Industrial CyberSecurity for Networks is installed.

Kaspersky Endpoint Agent does not analyze or send data on excluded application processes to the server with KATA Central Node or Kaspersky Industrial CyberSecurity for Networks installed.

Optimization of the volume of EDR telemetry about application processes can be managed (enabled / disabled) when Kaspersky Endpoint Agent is integrated with servers where Kaspersky Industrial CyberSecurity for Networks is installed.

If optimization of the volume of EDR telemtry is enabled, Kaspersky Endpoint Agent does not send events with 102 (basic communications) and 8 (network activity of a process) codes for the Microsoft SMB protocol and the Network Agent process klnagent.exe regarding processes of applications on a server where KATA Central Node or Kaspersky Industrial CyberSecurity for Networks is installed.

To enable and configure exclusions for and optimization of the volume of EDR telemetry on application processes:

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

- **Open the policy properties window**.

  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **EDR telemetry** section, select **Excluded processes**.

   The **Excluded processes** window opens.

3. In the **Exclusions** settings group, enable the **Use exclusions** setting to enable use of EDR telemetry exclusions.

4. Configure optimization of the volume of EDR telemetry:

   When Kaspersky Endpoint Agent is integrated with servers where KATA Central Node is installed, optimization of the volume of EDR telemetry should always be enabled.

   - Disable the **Optimize the amount of telemetry** setting if you want Kaspersky Endpoint Agent to send events with codes 102 (basic communications) and 8 (the process's network activity) for the Microsoft SMB protocol, WinRM service, and the Network Agent process klnagent.exe.
   - Enable the **Optimize the amount of telemetry** setting if you want Kaspersky Endpoint Agent to not send events with codes 102 (basic communications) and 8 (the process's network activity) for the Microsoft SMB protocol and the Network Agent process klnagent.exe.

   If the **Use exclusions** setting is disabled, Kaspersky Endpoint Agent does not send events with codes 102 (basic communications) and 8 (the process's network activity) for the Microsoft SMB protocol and the Network Agent process klnagent.exe, regardless of the value of the **Optimize the amount of telemetry** setting.

5. Create a list of exclusions:

   a. Click the **Add** button.

   b. In the **Rule properties** window that opens, **configure the exclusion settings**:

      Exclusion settings are applied using a logical AND.

      To create an exclusion, specify the value in the **Full path** field and select at least one event type in the **Use this exclusion for the following event types** list.

      If the **Network events** value is selected for the **Use this exclusion for the following event types** criterion, specify the full path to the file in the **Full path** field.

The object for which you create an exclusion must be available on the protected device at the time the exclusion settings are applied. For example, if you first configure exclusion for a specific application, and then install that application on the protected device, this exclusion will not be applied.

1. In the **Process information** section, specify the values in the following fields:
   - **Full path**. Full path to the file, including its name and extension. You can use file masks (using the ? and * characters), as well as system environment variables.
   - **Command line text**. Command line to run the object.
   - **Parent folder path**. The path to the folder where the file is located.
2. In the **File properties** section, specify the values in the following fields:
   - **File description**. The value of the FileDescription parameter from the resource of the RT_VERSION type (VersionInfo).
   - **Original file name**. The value of the OriginalFilename parameter from the resource of the RT_VERSION type (VersionInfo).
   - **File version**. The value of the FileVersion parameter from the resource of the RT_VERSION type (VersionInfo).
3. In the **File checksums** section, specify the values in the following fields:
   - **MD5**. MD5 hash of the file.
   - **SHA256**. SHA256 hash of the file.
4. In the **Use this exclusion for the following event types** list, select at least one value:
   - **File modification**.
   - **Network events**.
   - **Interactive input in the console**.

     This event type is selected by default.
   - **Loading the process module**.
   - **Changes in the Registry**.

c. Click **OK** to save the changes and close the **Rule properties** window.

The new exclusion is created and displayed in the list of exclusions.

d. If you need to export the exclusion list to an XML file, click the **Export** button.

e. If you need to import the exclusion list from an XML file, click the **Import** button.

f. If you need to modify an exclusion, click the **Modify** button.

g. If you need to delete an exclusion from the list, select the exclusion and click the **Delete** button.

6. If you are configuring the policy settings, make sure that the switch in the upper right corner of the group of settings is turned on. It is the default position of the switch.

7. Click **OK** to save the changes.

Enabling and configuring exclusions for sent EDR telemetry about network communications

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can configure exclusions for EDR telemetry about network communications using Kaspersky Security Center Web Console, in the properties of an individual device or in the policy settings for a group of devices.

Exclusions for EDR telemetry about network communications are applied when Kaspersky Endpoint Agent is integrated with servers where Kaspersky Industrial CyberSecurity for Networks is installed.

Kaspersky Endpoint Agent does not analyze or send data matching exclusion settings to the server with KATA Central Node or Kaspersky Industrial CyberSecurity for Networks installed.

To enable and configure EDR telemetry about network communications:

1. Do one of the following:

   - **Open the application properties window for an individual device**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
     2. Select the device.
     3. In the **<Device name>** window that opens, select the **Applications** tab.
     4. Select **Kaspersky Endpoint Agent**.
     5. In the window that opens, select the **Application settings** tab.

   - **Open the policy properties window**.

     1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
     2. Select the policy you want to configure.
     3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **EDR telemetry** section, select **Excluded network communications**.
   The **Excluded network communications of the process** window opens.

3. In the **Exclusions** settings group, enable the **Use exclusions** setting to enable use of EDR telemetry exclusions.

4. Create a list of exclusions:

   a. Click the **Add** button.

   b. In the **Rule properties** window that opens, **configure the exclusion settings.**

   > Exclusion settings are applied using a logical AND.

      1. In the **Name** field, enter the name of the exclusion.
      2. In the **Direction** drop-down list, select the direction of network traffic.
      3. In the **Protocol** drop-down list, select the network protocol.
      4. If you select a custom protocol, in the **Number** field, enter the network protocol number.
      5. Select the **Local port OR range** check box and enter the port number or number range.

         For incoming connections (in the **Direction** drop-down list, **Incoming** is selected), enter the port or range of ports for the local device.

         For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the port or range of ports for the remote device.

         The values 1–65535 are available for port numbers.

         The values 1–10, 20–30000 and 1–65535 are available for a range of ports.

         Limitations:

         - For network connections of a local device running the Windows XP operating system, you can specify only a single port, because Windows XP does not support a range of ports.
         - For network connections of a remote device running the Windows XP operating system, you can specify a range of ports, but only the first port in the specified range is correctly applied, because Windows XP does not support a range of ports.

      6. Select the **Remote port OR range** check box and enter the port number or number range.

         For incoming connections (in the **Direction** drop-down list, **Incoming** is selected), enter the port or range of ports for the remote device.

         For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the port or range of ports for the local device.

         The values 1–65535 are available for port numbers.

         The values 1–10, 20–30000 and 1–65535 are available for a range of ports.

Limitations:

- For network connections of a local device running the Windows XP operating system, you can specify only a single port, because Windows XP does not support a range of ports.
- For network connections of a remote device running the Windows XP operating system, you can specify a range of ports, but only the first port in the specified range is correctly applied, because Windows XP does not support a range of ports.

7. Select the **Local address** check box and enter the network address of the device for which Kaspersky Endpoint Agent will not analyze or send EDR telemetry about network traffic in accordance with the exclusion settings.

   For incoming exclusions (in the **Direction** drop-down list, **Incoming** is selected), enter the network address for the local device.

   For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the network address of the remote device.

   > For IP addresses, only addresses in IPv4 format are supported.

8. Select the **Remote address** check box and enter the network address of the device for which Kaspersky Endpoint Agent will not analyze or send EDR telemetry about network traffic in accordance with the exclusion settings.

   For incoming connections (in the **Direction** drop-down list, **Incoming** is selected), enter the network address for the remote device.

   For outgoing connections (in the **Direction** drop-down list, **Outgoing** is selected), enter the network address for the local device.

   > For IP addresses, only addresses in IPv4 format are supported.

9. **Create the list of application** for which Kaspersky Endpoint Agent will not analyze or send EDR telemetry about network traffic in accordance with the exclusion settings.

   1. Select the **Applications** check box.
   2. In the field below, specify the path to the executable file of the application you want to add to the list. You can enter the path manually or with the help of the **Browse** button.
   3. Click the **Add** button.
   4. For each application you want to add to the list, repeat steps 2 and 3 of the guide.
   5. If necessary, remove an application from the list:
      a. Select the application in the list.
      b. Click the **Delete** button.

10. Click **OK** to save the changes and close the **Rule properties** window.

    The new exclusion is created and displayed in the list of exclusions.

c. If you need to modify an exclusion, click the **Modify** button.

d. If you need to delete an exclusion, select the exclusion and click the **Delete** button.

5. If you are configuring the policy settings, make sure that the switch in the upper right corner of the group of settings is turned on. It is the default position of the switch.

6. Click **OK** to save the changes.

Configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Before performing the following steps, get the MDR configuration file. It contains a configuration file (BLOB) required for integration.

By downloading the Kaspersky Managed Detection and Response configuration file, you agree to automatically send the data from the device with Kaspersky Endpoint Security installed to Kaspersky for processing. Do not download the configuration file if you do not want the transmitted data to be processed.

If you want Kaspersky Endpoint Agent to process data about events generated by Kaspersky Industrial CyberSecurity for Networks and send this data to Kaspersky Managed Detection and Response, configure interaction with Kaspersky Security Center in the settings of Kaspersky Industrial CyberSecurity for Networks. For detailed information on configuring interaction between the applications, refer to the Kaspersky Industrial CyberSecurity for Networks documentation.

To configure integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response using the Kaspersky Security Center Web Console:

1. Open the Kaspersky Security Center Web Console.

2. Open the **Devices** → **Policies and profiles** tab.

3. In the list of policies, select the name of Kaspersky Endpoint Agent policy that you want to configure.

   This opens the policy settings window.

4. Enable **KSN Usage**.

   Open the main window of the Kaspersky Security Center Web Console.

5. In the Administration Console tree, configure the **Private KSN** settings (for information on configuring Kaspersky Security Network proxy server settings, refer to *Kaspersky Security Center Help*).

   Download the Kaspersky Managed Detection and Response configuration file with the pkcs7 extension that is included in the mdr_config.zip archive.

6. To continue configuring integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response, open the main window of the Kaspersky Security Center Web Console.

7. Open the **Devices** → **Policies and profiles** tab.

8. In the list of policies, select the name of Kaspersky Endpoint Agent policy that you want to configure.

   This opens the policy settings window.

9. On the **Application settings** tab, select **Managed Detection and Response**.

10. In the **Managed Detection and Response settings** group, do the following:

    a. Switch the toggle button to **Managed Detection and Response enabled**.

    b. Click the **Upload configuration file (BLOB)** button and select the BLOB configuration file to load.

    c. In the **User identifier** field, enter an arbitrary value.

    d. In the upper right corner of the settings group, change the switch from **Undefined** to **Enforce**.

11. Click **Save** to save the changes.

Integration between Kaspersky Endpoint Agent and Kaspersky Managed Detection and Response is configured.

MDR operation when using Kaspersky Endpoint Agent simultaneously with Kaspersky Endpoint Security

Kaspersky Endpoint Security 11 or later with the current database version supports interaction with MDR. In Kaspersky Endpoint Security 11.6.0 or later, interaction with MDR is available immediately after installation.

If you use Kaspersky Endpoint Agent to work with MDR and install Kaspersky Endpoint Security of the version that supports interaction with MDR or update Kaspersky Endpoint Security 11 or later databases to the current version, MDR stops working with Kaspersky Endpoint Agent and becomes available for work with Kaspersky Endpoint Security. At that:

- Switching between Kaspersky Endpoint Agent and Kaspersky Endpoint Security is performed in quiet mode.
- Kaspersky Endpoint Agent allows for configuring settings for interaction with MDR, but these settings are not applied on the device.
- If Kaspersky Endpoint Security is not available (for example, you uninstalled the application), MDR can start working with Kaspersky Endpoint Agent if you restart the Kaspersky Endpoint Agent service.
- The Managed Detection and Response component remains in the *Running* status in Kaspersky Endpoint Agent settings on the device, since Kaspersky Endpoint Agent continues to communicate with MDR (for example, to resume working with the solution if necessary).

Configuring storage settings in Kaspersky Endpoint Agent

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

This section describes how to configure the quarantine settings and data synchronization settings with the Administration Server by means of Kaspersky Endpoint Agent Management plug-in.

About Kaspersky Endpoint Agent quarantine

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Quarantine is a special local repository on the device. The user can put files considered dangerous to the computer into quarantine. 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 Network Agent 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can use Kaspersky Security Center to configure quarantine settings, view the properties of the quarantined objects on the protected devices, 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 documentation.

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.

Kaspersky Endpoint Agent quarantines object under the system account (SYSTEM).

Quarantined objects can be removed using 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure quarantine settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
2. Select the policy you want to configure.
3. In the **<Policy name>** window that opens, select the **Application settings** tab.
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 will be:
      `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 specify the maximum size of quarantine in megabytes 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 will publish the corresponding event on Kaspersky Security Center server and in the Windows Event Log, but will 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 will publish the corresponding event on the Kaspersky Security Center server and in the Windows Event Log, but will 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 will be:
`C:\ProgramData\Kaspersky Lab\Endpoint Agent\4.0\Restored`

7. If you configure the policy settings, in the upper right corner of the group of settings, change the switch from **Undefined** to **Enforce**.

8. Click **Apply** and **OK**.

The quarantine settings and the folder for restoring objects from quarantine have been configured.

Configuring data synchronization with the Administration Server

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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. Do one of the following:

- **Open the application properties window for an individual device**.

    1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.

    2. Select the device.

    3. In the **<Device name>** window that opens, select the **Applications** tab.

4. Select **Kaspersky Endpoint Agent**.
5. In the window that opens, select the **Application settings** tab.

- **Open the policy properties window**.
  1. In the main Kaspersky Security Center Web Console window select **Devices** → **Policies and profiles**.
  2. Select the policy you want to configure.
  3. In the **<Policy name>** window that opens, select the **Application settings** tab.

2. In the **Repositories** section select the **Synchronization with Administration Server** subsection.
3. Select the **Data about quarantined objects on managed devices**.
4. Click **OK**.
5. Click the **Save** button.

Data synchronization with the Administration Server is configured.

Configuring failure diagnosis

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent does not automatically create a folder for storing trace or dump files on the device. Specify a folder that is already available on the device.

To configure failure diagnosis:

1. **Open the application properties window for an individual device**.
   1. In the main Kaspersky Security Center Web Console window select **Devices** → **Managed devices**.
   2. Select the device.
   3. In the **<Device name>** window that opens, select the **Applications** tab.
   4. Select **Kaspersky Endpoint Agent**.
   5. In the window that opens, select the **Application settings** tab.
2. In the **Application settings** section select the **Failure diagnosis** subsection.

3. To enable logging of debug information to the trace files:

    a. Enable the **Write debug information to trace files** option.

    b. In the **Trace files folder** field, specify the path to the folder on the device where the application saves the trace files.

    > Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

    c. In the **Maximum trace file size (MB)** field, specify the file size in megabytes.

    The default value is 50 MB. When the specified file size is reached, the application continues writing to a new file.

4. If you want the application to overwrite old trace files:

    a. Enable the **Overwrite old trace files** option.

    b. Enter the desired value in the **Maximum number of files per trace log** field.

    The default value is 1 file. When the specified number of files is reached, the application overwrites old files, starting with the oldest one. The specified limit is applied separately for each Kaspersky Endpoint Agent process being debugged, so the total number of files for all processes may exceed the specified value.

5. To enable logging of dump files:

    a. Enable the **Create dump files** option.

    b. In the **Dump files folder** field, specify the folder to save the dump files.

    > Make sure that the specified folder is available on the managed device. Otherwise, the debug information will not be saved.

6. Click **OK**.

Failure diagnostics is configured and enabled for all Kaspersky Endpoint Agent processes that are currently running. Failure diagnostics files will be generated in the folders you specified.

Managing Kaspersky Endpoint Agent tasks

This section describes how to manage Kaspersky Endpoint Agent tasks.

Creating tasks

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To create a task:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. Click the **Add** button.

   The task creation wizard will start.
3. In the **Application** drop-down list, select **Kaspersky Endpoint Agent**.
4. In the **Task type** drop-down list, select the required task type and follow the wizard instructions.
5. To change the default values of the task settings immediately after its creation, select the **Open task details when creation is complete** check box on the **Finish task creation** page.

   If you do not select this check box, the task will be created with the default settings. You can subsequently change these settings at any time for the following task types:

   - Application activation
   - IOC Scan
   - Security audit
   - Delete file
   - Quarantine file
   - Terminate process
   - Run process
   - Application Databases and Modules Update
6. Click **Finish**.

The task will be created and displayed in the list of tasks.

You can start the created task manually or configure a scheduled task start.

Viewing the table of tasks

To view the list of tasks,

select **Devices** → **Tasks** in the main Web Console window.

A list of tasks appears. The tasks are grouped by the names of the applications for which they are created.

Deleting a task from the list

To remove tasks from the list of tasks on Kaspersky Security Center server:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
   A list of tasks appears.
2. In the list of tasks, select the check boxes next to the tasks that you want to delete.
3. Click the **Delete** button.
   The action confirmation window opens.
4. Click **Yes**.

The selected tasks will be deleted from the list.

Configuring task schedule settings

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the scheduled task start:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. On the **Schedule** tab in the **General** section, change the toggle button from **Schedule disabled** to **Run by schedule**.
4. In the **Frequency** drop-down list select one of the following options: **At specified time**, **Every hour**, **Every day**, **Every week** or **On application launch**.
5. If you select the **At specified time** option, specify the day and time to start the task.

6. If you select one of the following options: **Every hour**, **Every day** or **Every week**, configure the following settings:

    a. In the **Every** field, specify 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** fields, select the date and time from which the schedule applies.

7. To configure advanced schedule settings, select the **Advanced** section and perform the following steps:

    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 the 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 devices to the Administration Server as well as to run the task on workstations not precisely according to the schedule, but randomly within a certain time interval, select the **Randomize the task start time within the interval** check box and specify the start interval in minutes.

8. Click the **Save** button.

Starting tasks manually

The application starts tasks according to the schedule specified in the properties of each task. You can start the task manually at any time.

To start a task manually:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.

2. In the list of tasks, select the check box next to the task that you want to start.

3. Click **Start**.

The task will be started. You can check the task status in the **Status** column or by clicking the **Result** button.

Creating Kaspersky Endpoint Agent activation tasks

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can activate Kaspersky Endpoint Agent using a license key from the Kaspersky Security Center key store. For detailed information on managing license keys using Kaspersky Security Center, refer to the *Kaspersky Security Center Help*.

To create Kaspersky Endpoint Agent activation task:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. Click the **Add** button.

   The task creation wizard will start.
3. In the **Application** drop-down list, select **Kaspersky Endpoint Agent**.
4. In the **Task type** drop-down list, select **Application activation**.
5. In the **Task name** field, specify the display name of the task.
6. To create a task for devices of a specific Administration Server group, perform the following actions:
   a. In the **Selecting devices to which the task is assigned** group of settings, select the **Group of devices** option and click **Next**.
   b. Select the desired Administration Server group and click **Next**.
7. To create a task for specific devices using a range of IP addresses, NetBIOS names, DNS names, or to select devices from the list of devices detected in the network by the Administration Server, perform the following actions:
   a. In the **Selecting devices to which the task is assigned** group of settings, select the **Selected or imported from the list** option and click **Next**.
   b. Add devices to the list by the required criteria and click **Next**.
8. To create a task for devices of a specific selection, perform the following actions:
   a. In the **Selecting devices to which the task is assigned** group of settings, select the **Selection** option and click **Next**.
   b. Select the desired selection from the list and click **Next**.
9. In the **Select a license key** window, select the required license key from the list of Kaspersky Security Center keys available in the key storage.
10. If you want to add this license key as an additional one to automatically renew the license, select the **Use as additional key** check box.
11. Click **Next**.
12. In the **Selecting an account to run a task** window, select the desired account and click **Next**.

13. To change the default values of the task settings immediately after its creation, select the **Open task details when creation is complete** check box on the **Finish task creation** page.

14. Click **Finish**.

    The task will be created and displayed in the list of tasks.

    You can start the created task manually or configure a scheduled task start.

Configuring Database and application module update task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Database and application module update task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. Select the **Connection settings** section.
5. If you use Kaspersky Security Center, in the **Update source** group of settings, select one of the following options:
   - **Kaspersky Security Center Administration Server**.
   - **Kaspersky update servers**.
   - **Custom HTTP or FTP servers or network folders**.
6. If you use Kaspersky Security Center Cloud Console, in the **Update source** group of settings, select one of the following options:
   - **Distribution points**. Devices with Network Agent installed are used as the update source.

     Detailed information on using the distribution points is available in the Kaspersky Security Center Cloud Console Help.
   - **Kaspersky update servers**. Kaspersky update servers are used as the update source.

7. If required, select the **Use Kaspersky update servers if specified servers are not available** check box.

   Not available in Kaspersky Security Center Cloud Console.

8. If you select **Custom HTTP or FTP servers or network folders** as database update source, do the following:

   Not available in Kaspersky Security Center Cloud Console.

   a. Click the **Settings** link to open the **Custom update sources** window.

   b. Add the update sources to the list by following these steps:

      1. Click the **Add** button.
      2. In the dialog box that opens, in the **Web address** field, enter the address of the update server (HTTP or FTP), or the path to the network folder or local folder containing the update files, and click **OK**.
      3. If you want to use the database update source, switch the toggle button next to its address to **Enable**.

         Follow the same steps to add each update source.

      4. Click **OK**.

         The **Custom update sources** window closes.

9. Select the **Update settings** section.
10. In the **Update settings** section, select the conditions for the application to check for the availability of application module updates:

    - **Do not check for updates**. Kaspersky Endpoint Agent will not check the availability of application module updates.
    - **Only check for availability of critical software modules updates**. Kaspersky Endpoint Agent will check the availability only for important application module updates.
    - **Download and install critical software modules updates**. Kaspersky Endpoint Agent will check the availability of application module updates and download and install critical application module updates.

11. 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 application module updates** check box.
12. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

Managing Standard IOC Scan tasks

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Standard IOC Scan tasks are group or local tasks that are created and configured manually in Kaspersky Security Center or through the command line interface. IOC files prepared by the user are used to run the tasks.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

This section provides instructions on how to manage Standard IOC Scan tasks.

Requirements for IOC files

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

When creating IOC Scan tasks, consider the following requirements and limitations related to 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.
- Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.
- 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.
- The size of a single IOC file must not exceed 3 MB. Using larger files results in the failure of IOC Scan tasks. In this case, the total size of all added files in the IOC collection can exceed 3 MB.
- It is recommended to create one IOC file per each threat. This makes it easier to read the results of the IOC Scan task.

The table below shows the features and limitations of the OpenIOC standard supported by the application.

Features and limitations of the OpenIOC standard versions 1.0 and 1.1

Supported conditions	OpenIOC 1.0:
	
	`is`
	`isnot` (as an exclusion from the set)
	`contains`
	`containsnot` (as an exclusion from the set)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

Supported condition attributes	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

Supported operators	`AND` `OR`
Supported data types	`date`: date (applicable conditions: `is`, `greater-than`, `less-than`) `int`: integer number (applicable conditions: `is`, `greater-than`, `less-than`) `string`: string (applicable conditions: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `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`.
	
	The application supports interpretation of the `Content` parameter specified as intervals for the following data types: `int` and `date`:
	
	OpenIOC 1.0:
	Using the `TO` operator in the `Content` field:
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	Using the `greater-than` and `less-than` conditions
	Using the `TO` operator in the `Content` field
	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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

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

Configuring Standard IOC Scan task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

To configure the Standard IOC Scan task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. In the **IOC scan settings** section, configure the IOC collection by following these steps:
   a. In the **IOC collection** group of settings click the **Redefine IOC files** button.
   b. In the dialog that opens, click the **Add IOC files** button and specify the IOC files that you want to use for the task.
      You can select multiple IOC files for a single IOC Scan task.
   c. Click **OK** to close the dialog box.

      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.

   d. To view the list of all IOC files that are included in the IOC collection, as well as to obtain information about each IOC file, do the following:
      1. Click the link with the names of all downloaded IOC files in the **IOC files** group of settings.
         The **IOC contents** window opens.
      2. To view detailed information about an individual IOC file, click the name of the required IOC file in the list of files on the **IOC collection** tab.
         In the window that opens, information about the selected IOC file will be displayed.

3. To close the window with information about the selected IOC file, click **OK** or **Cancel**.

4. To view information about all downloaded IOC files at once, open the **IOC data** tab.

   Information about each downloaded IOC file will be displayed in the workspace of the window.

5. If you do not want to use a specific IOC file when the IOC Scan task is executed, on the **IOC collection tab**, switch the toggle button next to the IOC file name from **Include** to **Exclude**.

6. Click **OK** to save the changes and close the **IOC contents** window.

e. To export the created IOC collection, click the **Export IOC collection** button.

   In the window that opens, specify the name of the file and select the folder where you want to save it.

f. Click the **Save** button.

   The application creates a ZIP file in the specified folder.

g. In the **Retrospective IOC scan** group of settings configure the settings for Retrospective IOC scan mode:

1. In the **Retrospective IOC Scan** group of settings enable the **Perform Retrospective IOC Scan within the interval** option.

2. Specify the time interval.

   During the task execution, the application analyzes data collected during the specified time interval, including the boundaries of the specified interval (from 00:00 on the start date until 23:59 on the end date). The default interval starts at 00:00 on the day preceding the task creation day and ends at 23:59 on the day when the task was created.

   > If during execution of the IOC Scan task with the **Perform Retrospective IOC Scan within the interval** option enabled the application does not find any data for the specified time interval to be analyzed, it does not inform about this. In this case, the application shows no indicators of compromise in the task completion report.

h. In the **Actions** group of settings, configure the response actions on detecting the indicator of compromise:

1. Select the **Take response actions after an indicator of compromise is found** 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 **Quarantine and delete** check box to quarantine the detected object and remove it from the device.

4. Select the **Run critical areas scan on the device** 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.

> If the **Quarantine and delete** or **Run critical areas scan** option is enabled, Kaspersky Endpoint Agent may recognize the detected files as infected and delete them from the device in response.

i. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to protect critical system files from being quarantined or deleted when an indicator of compromise is detected.

The option is available only if the **Quarantine and delete** option is selected in the **Actions** group of settings.

If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.

5. In the **Advanced** section, select data types (IOC documents) that you want to analyze during the task execution and configure the additional scan settings:

   a. In the **Select data types (IOC documents) to analyze during IOC scanning** group of settings, select the check boxes next to the required IOC documents.

   Depending on the loaded IOC files, some check boxes may be disabled.

   Kaspersky Endpoint Agent automatically selects data types (IOC documents) for the IOC Scan task in accordance to the contents of the downloaded IOC files. It is not recommended to unselect data types manually.

   b. If the **Analyze file data (FileItem)** check box is selected, click the **Advanced (FileItem)** link and in the **FileItem document scan settings** window that opens, select the scan areas on the protected device drives where to look for indicators of compromise.

   You can select one of the predefined areas, or specify the paths to the desired areas manually.

   c. Click **OK** to save the changes and close the **FileItem document scan settings** window.

   d. If the **Analyze WEL data (EventLogItem)** check box is selected, click the **Advanced (EventLogItem)** link and in the **EventLogItem document scan settings** window that opens, configure additional event analysis settings:

   - **Scan only events that are logged within the specified period**.

     If the check box is selected, only the events that were logged during the specified period will be taken into account during the task's execution.

   - **Scan events that belong to the following channels**.

     List of channels to be analyzed during the task's execution.

   e. Click **OK** to save the changes and close the **FileItem document scan settings** window.

6. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

Viewing IOC Scan task execution results

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To view the IOC Scan task execution results:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. Select the **IOC Scan results** section.
5. In the **Device** drop-down list, select the devices, for which you want to view the results of IOC Scan task.

   A summary table with the task execution results on the selected devices will be displayed.

   If compromise indicators are detected on devices, the **Results** column displays the *compromise indicators detected* link.
6. If you want to view detailed information on the detected compromise indicators on a specific device, do the following:

   a. Click the **compromise indicators detected** link in the row with the name of the desired device.

      The **IOC Scan results** window opens that contains a list of all IOC files used in the task. If there is an object on the selected device that matches a certain compromise indicator, the **Status** column displays the *Match* value.

   b. Click the **Match** link in the row with the name of the desired IOC file.

      The **IOC incident card** window opens.

      The *IOC incident card* contains information about objects on the device 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 IOC incident card is not available for IOC files for which no matches were detected on the device during scanning.

Configuring the Quarantine file task

> This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you suspect that an infected or probably infected file is on the computer, you can isolate it by moving it to quarantine.

> Task creation is performed before, as an individual step.

> If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Quarantine file task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. In the **Specify the file to be Quarantined** drop-down list, select one of the following values: **Specify the file by full path** or **Specify the file by folder path and checksum**.
5. If you select the **Specify the file by its full path** option, specify the value in the **File full path** field.
6. If you select the **Specify the file by folder path and checksum** option, configure the following settings:
   - In the **Checksum type** drop-down list, select one of the following values: **MD5** or **SHA256**.
   - Specify the value in the **File checksum** field.
   - Specify the value in the **File folder path** field.
7. In the **Actions after quarantining file** group of settings, select whether the file must be deleted from the protected device after quarantining.

   If the file is locked by another process, the file will only be deleted after the device has been rebooted.

8. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the task scope.

   If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.

9. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

If the file is locked by another process, the task will be displayed with the *Completed* status, but the file itself will only be quarantined after the device has been restarted. It is recommended to check whether the task was completed successfully after the device has been restarted.

The Quarantine file task may fail with the *Access denied* error if you try to quarantine an executable file that is currently running. To solve this problem, create the Terminate process task for this file and try to create a Quarantine file task again.

Configuring the Delete file task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Delete file task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. In the **File to delete** list, click the **Add** button.
5. The **File to delete** dialog box opens.
6. In the **Specify the file to delete** drop-down list, select one of the following values: **Specify the file by its full path** or **Specify the file by its folder path and checksum**.
7. If you select the **Specify the file by its full path** option, specify the value in the **File full path** field.
8. If you select the **Specify the file by folder path and checksum** option, configure the following settings:
   - In the **Checksum type** drop-down list, select one of the following values: **MD5** or **SHA256**.
   - Specify the value in the **File checksum** field.
   - Specify the value in the **File folder path** field.
   - Select the **Including subfolders** check box for the application to delete all occurrences of the object not only in the specified folder, but also in all its subfolders.
9. Click **OK** to add the specified object to the **File to be removed** list.

   You can specify several objects for deletion in one Delete file task.

10. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the task scope.

    If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.

11. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

If the file is locked by another process, the task will be displayed with the *Completed* status, but the file itself will only be deleted after the device has been restarted. It is recommended to check whether the file was deleted successfully after the device has been restarted.

Deleting a file from a connected network drive is not supported.

Configuring the Run process task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Using the Run process task, you can run the required application or command on the device.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Run process task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. To run the application using the command line (cmd.exe) or execute a command, type the required command in the **Executable command** field.

5. If you want to run the application directly, do the following:

   a. Specify the path to the application executable file in the **Working folder** field.

   b. Specify the keys for running the application in the **Arguments** field.

6. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

Configuring the Terminate process task

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

If you believe that a process running on the device could threaten the security of the device or the corporate LAN, you can terminate the process.

Task creation is performed before, as an individual step.

If you selected the **Open task details when creation is complete** check box on the **Finish task creation** page during the task creation, proceed to step 4 of the following instruction.

To configure the Terminate process task settings:

1. In the main Kaspersky Security Center Web Console window select **Devices** → **Tasks**.
2. To open the task settings window, click the task name.
3. Select the **Application settings** tab.
4. In the **File full path** field specify the path to the file of the process that you want to terminate.
5. In the **Checksum type** drop-down list, select one of the following values: **Not specified**, **MD5** or **SHA256**.
6. If you select **MD5** or **SHA256**, specify the value in the **Checksum** field.
7. If you want the application to consider the character case in the path to the process file, select the **Path is case sensitive** check box.
8. In the **Protection of critical system files** group of settings, select the **Do not perform actions on critical system files** check box if you want to exclude critical system files from the task scope.

   If this option is selected and an object is a critical system file, the application does not perform any actions on this object. This information is logged in the task execution report.

9. Click the **Save** button.

You can start the created task manually or configure a scheduled task start.

Managing Kaspersky Endpoint Agent using the command line interface

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent can be managed using 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 the Kaspersky Endpoint Agent distribution kit and is installed on each device together with Kaspersky Endpoint Agent. It is installed in the `%ProgramFiles%\Kaspersky Lab\Endpoint Agent` folder (if a 32-bit operating system is used on the device) or in the `% ProgramFiles(x86)%\Kaspersky Lab\Endpoint Agent` folder (if 64-bit operating system is used on the device).

Example:
If the device has the x64 Windows operating system installed and you select the C Drive as the installation location for Kaspersky Endpoint Agent, the Agent.exe utility will be placed in the following folder:
`C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\`

To manage Kaspersky Endpoint Agent using 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, enter the 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) will be displayed.

To display help on all the application settings and their possible values,

run the following command: `agent.exe --help`

Managing Kaspersky Endpoint Agent activation

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage application activation 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, enter the 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 an 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:

- `-305` – the added key has expired.
- `2` – undefined application error.
- `-302` – the added key is in the deny list.
- `-301` – the added key is not suitable to activate Kaspersky Endpoint Agent.
- `-303` – key file is damaged.
- `4` – syntax errors.
- `-304` – invalid path to the key file has been specified.

Managing Kaspersky Endpoint Agent authentication

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage application authentication using 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 --proxy={enable|disable|show} --mode={auto|custom} --server=<proxy server address> --port=<port number> --use-auth={yes|no} --proxy-user=<user name> --proxy-password=<user password> --bypass-local={yes|no}`

The authentication parameters are described in the following table.

Authentication parameters

Parameters	Description
`--proxy={enable|disable|show}`	Required parameter. This parameter controls the connection to the proxy server. The following values are available: `enable` – enables proxy server usage. `disable` – disables proxy server usage. `show` – displays the current proxy server usage settings. The specified proxy server will be used to work with Kaspersky Security Network and to update databases. The settings of the specified proxy server can be used for integration with other statistics collection systems. The use of the specified proxy server must be separately enabled in the integration settings.

--mode={auto|custom}	Required parameter. This parameter sets the proxy server configuration mode. The following values are available: `auto` – automatic detection of the proxy server. `custom` – manual configuration of the proxy server access parameters.
--server=< proxy server address >	Required parameter. Specifies the proxy server address.
--port=<port port number >	Required parameter. Specifies the proxy server connection port.
--use-auth={yes|no}	Optional parameter. This parameter indicates whether proxy server authentication is required. The following values are available: `yes` – user name and password must be specified to connect to the proxy server. `no` – connection to the proxy server is possible without specifying a user name and password. Used by default.
--proxy-user=<user user name >	Optional parameter. Specifies the user name to connect to the proxy server. Empty by default.
--proxy-password=< user password >	Optional parameter. Specifies the password to connect to the proxy server. Empty by default.
--bypass-local={yes|no}	Optional parameter. This parameter toggles a direct connection to local addresses without using a proxy server. Available values: `yes` – connections to the addresses of the current local network will be established without a proxy server. Used by default. `no` – connections to the addresses of the current local network and to external addresses will be established through a proxy server.

Configuring tracing

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Kaspersky Endpoint Agent does not automatically create a folder for storing trace or dump files on the device. Specify a folder that is already available on the device.

To configure tracing in Kaspersky Endpoint Agent using 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, enter the 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 the trace files are to be saved>` 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.

     > Make sure that the specified folder is available on the managed device. Otherwise, trace files will not be created.

   - `agent.exe --trace=enable --folder <path to the folder where the trace files are to be saved> --rotation=yes --rotate-file-size=<maximum file size, MB> --rotate-files-count=<maximum number of files>`, enables tracing with overwriting old trace files when the values specified for the size and number of the trace files are reached.

     The specified limit on the number of files is applied separately for each Kaspersky Endpoint Agent process being debugged, so the total number of files for all processes may exceed the specified value. If you do not specify the `--rotate-file-size` or `--rotate-files-count` parameters (one or both) with the `--rotation=yes` parameter, the application uses the default values. The default value is 1 file of 50 MB.

   - `agent.exe --trace=disable` disables tracing.

     Tracing will be disabled for all Kaspersky Endpoint Agent processes that are currently running.

   - `agent.exe --trace=show` shows 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 will be displayed.

Return codes of the `--trace` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – 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 creating a dump of Kaspersky Endpoint Agent processes

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To configure the creation of dump files of Kaspersky Endpoint Agent processes using 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, enter the 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>` enables the creation of dump files of Kaspersky Endpoint Agent processes.

     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.

     Make sure that the specified folder is available on the managed device. Otherwise, dump files will not be created.

   - `agent.exe --dump=disable` disables dump creation.

     Creation of dump files will be disabled for all Kaspersky Endpoint Agent processes that are currently running.

   - `agent.exe --dump=show` shows 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 will be displayed.

Return codes of the `--dump` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

- 5 – object not found (unable to find the specified path to the dump files folder).
- 9 – invalid operation (for example, an attempt to execute the `--dump=disable` command, if the creation of dumps is already disabled).

Viewing information about quarantine settings and quarantined objects

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To view information about the quarantine settings and quarantined objects using 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, enter the 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>]` shows a list of quarantined objects.

   The following information will be displayed for all objects in the Quarantine folder on devices (the Quarantine folder is specified when quarantine settings are configured):

   - Identifiers of objects quarantined so far (`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).
   - Account of the user whose permissions were used to run the task to quarantine 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 found** global action.
     - `CUSTOM` if the file was quarantined manually as a result of execution of the `--quarantine=add` command.

- 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 as part of the 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 found** global action.
  - `BY USER` if the file was quarantined manually as a result of execution of the `--quarantine=add` command.
- `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 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

Actions on quarantined objects

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To perform actions on quarantined objects in Kaspersky Endpoint Agent using 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, enter the command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Do the following and press **ENTER**:
   - To permanently delete 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 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 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. Displayed when viewing information about quarantined objects (command `--quarantine=show`).
`--path-type=<original|custom|settings>`	The parameter describes the logic for destination folder selection when restoring objects from quarantine. • 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. • 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. • If the parameter is passed with the `<settings>` value, the object will be restored to the folder specified when quarantine settings were configured. If the folder is not available, the task fails. • If the parameter is passed with the `<custom>` value, the object will be restored to the folder whose path 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. This parameter defines the path to a folder for objects restored from quarantine if you do not want to use the folder where the object was located before being quarantined or the folder specified when quarantine settings were configured.
`--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 the same name as the file you are restoring from quarantine. • If the parameter is not passed, the restored object will be renamed: the `_restored` suffix will be added to the original object name. • 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. • 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>`	A required parameter if the `--hashalg` parameter is not passed. This parameter defines the full path to the object that you want to quarantine.
`--hashalg=<md5|sha256>`	A required parameter if the `--file` parameter is not passed and the full path to the object you want to quarantine is not specified. The parameter defines the hashing algorithm to calculate the checksum of the object you want to quarantine. The parameter can be passed with one of the following values: `<md5>` or `<sha256>`.

`--hash=<file checksum>`	Required parameter if the `--hashalg` parameter is passed. The parameter defines the checksum of the object you want to quarantine.
`--file=<folder that contains the file>`	Required parameter if the `--hashalg` parameter is passed. This parameter specifies the path to the folder that 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 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

Managing integration settings with KATA Central Node component

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage the integration settings of Kaspersky Endpoint Agent with the KATA Central Node component using 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, enter the 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> --use-proxy={yes|no} --compression=<yes|no> --partitioning-strategy=<automatic|user> [--message-key=<` message key `> --topic=<` topic `> --partition=<user specific partition>] --tls=<yes|no> --servers=<` address `>:<` port `>[;<` 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 integration settings between Kaspersky Endpoint Agent and the KATA Central Node component

Parameter	Description
`--message-broker=<enable|disable|show>`	Required parameter. Allows you to enable, disable, and view the status of the integration between Kaspersky Endpoint Agent and the KATA Central Node component. • `--message-broker=<enable>` – enables integration. • `--message-broker=<disable>` – disables integration. • `--message-broker=<show>` – displays the integration status of Kaspersky Endpoint Agent with the KATA Central Node component.
`--type=<kata>`	Required parameter. Allows you to specify the KATA Central Node component in order to manage the integration settings of Kaspersky Endpoint Agent with said component.
`--use-proxy={yes|no}`	Required parameter. Allows you to enable or disable proxy server usage in the message broker to send messages to KATA.
`--compression=<yes|no>`	Optional parameter. Allows you to enable or disable the compression of data transferred between Kaspersky Endpoint Agent and KATA Central Node. Enabled by default.
`---tls=<yes|no>`	Optional parameter. Allows you to enable or disable a trusted connection between Kaspersky Endpoint Agent and the KATA Central Node component. • `--tls=<yes>` – enables trusted connection. • `--tls=<no>` – disables trusted connection.
`--servers=<`address`>:<`port`>[;` <address>`:<`port`>[; …]]`	Required parameter. Allows the addition of one or more KATA servers. Kaspersky Endpoint Agent connects to the first server in the list. If the connection does not succeed, Kaspersky Endpoint Agent connects to the second server and so on down the list.
`--timeout=<` maximum response timeout of KATA server >	Optional parameter. Allows you to set the maximum response timeout of the 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. Allows you to add a TLS certificate for connecting Kaspersky Endpoint Agent to the KATA server.
`--client-certificate=<` full path to the certificate file >	Allows you to add a user certificate for connecting Kaspersky Endpoint Agent to the KATA server.
`--client-password= <password for the PFX archive>`	Allows you to enter a password for the PFX archive that contains the user certificate for connecting Kaspersky Endpoint Agent to the KATA server.
`--sync-period=<` interval for sending synchronization requests >	Allows you to specify the time interval for sending synchronization requests for Kaspersky Endpoint Agent settings and tasks with the KATA Central Node.
`--throttling=`<yes|no>	Allows you to enable or disable request throttling. The request throttling feature allows restricting the flow of events with low importance from Kaspersky Endpoint Agent to the Central Node component.
`--event-limit=`<number of events per hour>	Allows you to specify the maximum number of events per hour. The application analyzes telemetry data flow and restricts transmission of events with low importance if the number of transmitted events tends to exceed the specified value.
`--exceed-limit=`<threshold value>	Allows you to specify the threshold for exceeding the limit of events. If the flow of events with low importance of the same type exceeds the threshold percentage of the total number of events, the transmission of events of this type will be restricted. You can specify a value from 5 to 100 (without the % character).

Running Kaspersky Endpoint Agent database and module update

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To update the Kaspersky Endpoint Agent application database and modules using 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, enter the 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 spaces>|kl|ksc]
   ```

   Command parameters when running Kaspersky Endpoint Agent database update

Parameter	Description
`--update=bases|modules`	Required parameter. Allows you to specify the type of update: • `--update=bases` starts the application database update. • `--update=modules` starts the application module update.
`--source=<addresses of custom database update sources>|kl|ksc]`	Optional parameter. Allows you to select a database update source. • `--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. You can specify several addresses of custom database update sources, separated by semicolons without spaces (";"). The application will download updates from the first available database update source. If no addresses are available, the task will fail. • `--source=kl` allows you to select the **Kaspersky update servers** option as database update source. If the servers are not available, the task will fail. • `--source=ksc` allows you to select the **Kaspersky Security Center Administration Server** option as database update source. If the Administration Server is not available, the task will fail.

Return codes of the `--update=bases` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To start, stop, or view the current Kaspersky Endpoint Agent status using 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, enter the 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. • `--product=<start>` – starts the application. • `--product=<stop>` – stops the application. If password protection is configured for the application, a password is required to execute the `--product=<stop>` command. • `--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 – command is not supported.
- 0 – command successfully executed.
- 1 – 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To restrict Kaspersky Endpoint Agent's operations that might result in a decrease in the protection level of the user's computer and the data processed on that computer, as well as a decrease in the application's self-defense level, it is necessary to password protect the application.

The 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 to Kaspersky Sandbox>`
- `--quarantine=delete –ouid`
- `--quarantine=show`
- `--quarantine=restore`
- `--quarantine=add`
- `--product=stop`
- `--password=reset`
- `--isolation=disable`
- `--prevention=disable`
- `--selfdefense`
- `--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
- Application update (`upgrade`)
- Application repair (`repair`)
- Operations in the application installation wizard
- Operations in the command line interface

After enabling password protection and applying the Kaspersky Security Center policy, the same password is applied to all devices in the Kaspersky Endpoint Agent managed group.

After disabling password protection in the policy, the password protection settings are retained 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 using 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, enter the 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=state` 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

The protection of application services using the *Protected Process Light (PPL)* technology is implemented in Kaspersky Endpoint Agent.

The protection of application services using the Protected Process Light (PPL) technology is only available on the following operating systems:

- For workstations: Windows 10 version 1703 RS2 and above
- For servers: Windows Server 2016 version 1709 and above

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 using 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, enter the 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>]` shows the current status of application services protection by the PPL technology.
   - `agent.exe --ppl=disable [--pwd=<current user password>]` disables 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

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage self-defense settings using the Kaspersky Endpoint Agent 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, enter the command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.
3. Run the following command and press **ENTER**:

   ```
   agent.exe --selfdefense=<enable|disable>
   ```

Managing event filtering

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

To manage event filtering using the Kaspersky Endpoint Agent 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, enter the 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 Standard IOC Scan tasks

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

Standard IOC Scan tasks are group or local tasks that are created and configured manually in Kaspersky Security Center or through the command line interface. IOC files prepared by the user are used to run the tasks.

Only the files with IOC rules can be specified for the IOC Scan task. Files with other types of rules are not supported for the IOC Scan task.

To create and configure a Standard IOC Scan task using 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, enter the 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] [--network=no] [--url=no] [--drives=<all|system|critical|custom>] [--excludes=< list of exclusions >][--scope=< configurable list of folders >] [--retro]`

   If the `--scan-ioc` command is passed with only the required parameters, Kaspersky Endpoint Agent will perform the scan with the default settings.

   If the `--scan-ioc` command is passed together with the two required parameters (`--path=< path to the folder with IOC files >` and `< full path to the IOC file >`), Kaspersky Endpoint Agent scans the submitted IOC files.

Command parameters for running and configuring Standard IOC Scan tasks

Parameters	Description
`--scan-ioc`	Required parameter. 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. 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 ioc or xml extension, that you want to scan. A required parameter if the `--path=< path to the folder with IOC files >` parameter is not specified. Passed without the `--path` argument.

`--process=<no>`	Optional parameter. This parameter disables the analysis of process data during scans. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent does not consider the processes running on the device during scanning. If the IOC file contains IOC terms of the ProcessItem IOC document, they are ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scan the process data if the ProcessItem IOC document is described in the IOC file submitted for scanning.
`--hint=< full path to the process executable file | full path to the file >`	Optional parameter. This parameter allows you to narrow the scope of data analyzed while checking the ProcessItem and FileItem IOC documents by specifying a particular file. The parameter value can be set as: • `< full path to the executable file of the process >` – ProcessItem • `< full path to the file >` – FileItem This parameter can only be passed together with the `--process=yes` and `--files=yes` arguments.
`--dnsentry=no`	Optional parameter. This parameter disables the analysis of data on records in the local DNS cache (DnsEntryItem IOC document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not scan the local DNS cache. If the IOC file contains the terms of the DnsEntryItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scan the local DNS cache if the DnsEntryItem IOC document is described in the IOC file submitted for scanning.
`--arpentry=no`	Optional parameter. This parameter disables the analysis of data in ARP table (ArpEntryItem document) records during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not scan the ARP table. If the IOC file contains the terms of the ArpEntryItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scan the ARP table if the ArpEntryItem IOC document is described in the IOC file submitted for scan.
`--ports=no`	Optional parameter. This parameter disables the analysis of data on ports that are open for listening (PortItem document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not scan the table of active connections on the device. If the IOC file contains the terms of the PortItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scan the table of active connections if the PortItem IOC document is described in the IOC file submitted for scanning.
`--services=no`	Optional parameter. This parameter disables the analysis of data on services installed on the device (ServiceItem document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not scan data on services installed on the device. If the IOC file contains the terms of the ServiceItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scans the data on services if the ServiceItem IOC document is described in the IOC file submitted for scanning.
`--volumes=no`	Optional parameter. This parameter disables the analysis of volume data (VolumeItem document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not scan volume data on the device. If the IOC file contains the terms of the VolumeItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scan the data on volumes if the VolumeItem IOC document is described in the IOC file submitted for scanning.

`--eventlog=no`	Optional parameter. This parameter disables the analysis of data about Windows Event Log entries (EventLogItem document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not scan Windows Event Log entries. If the IOC file contains the terms of the EventLogItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only scan Windows Event Log entries if the EventLogItem IOC document is described in the IOC file submitted for scanning.
`--datetime=< event publication date >`	Optional parameter. This parameter allows you to enable or disable accounting for the date and time when the event was registered in the Windows Event Log when determining the IOC scan area for the corresponding IOC document. During IOC scanning, Kaspersky Endpoint Agent will only process events that were registered within the time interval between the specified date and time and the task execution time. Kaspersky Endpoint Agent allows you to specify the event registration date as the parameter value. Scans will be performed only for events registered in the Windows Event Log between the specified date and the time when the IOC scan is performed. If the parameter is not passed, Kaspersky Endpoint Agent will scan events with any registration date. The TaskSettings::BaseSettings::EventLogItem::datetime parameter cannot be changed. This parameter is only used if the EventLogItem IOC document is described in the IOC file submitted for scanning.
`--channel=< list of channels >`	Optional parameter. This parameter allows you to pass a list of the names of channels (logs) for which IOC scanning is required. If this parameter is passed, Kaspersky Endpoint Agent will only consider events published in the specified logs when performing the IOC Scan task. The name of the log is specified as a string based on 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). By default (including in the case that the parameter is not passed), IOC scanning is performed for the Application, System, and Security channels. Several values, separated by spaces, can be passed to the parameter. This parameter is only used if the EventLogItem IOC document is described in the IOC submitted for scanning.
`--system=no`	Optional parameter. This parameter disables the analysis of environmental data (SystemInfoItem IOC document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not analyze environmental data. If the IOC file contains the terms of the SystemInfoItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only analyze environmental data if the SystemInfoItem IOC document is described in the IOC file submitted for scanning.
`--users=no`	Optional parameter. This parameter disables the analysis of user data (UserItem IOC document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not analyze the data on users created in the system. If the IOC file contains the terms of the UserItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only analyze data on users created in the system if the UserItem IOC document is described in the IOC file submitted for scanning.
`--files=no`	Optional parameter. This parameter disables the analysis of data on files (FileItem IOC document) during IOC scanning. If the parameter is passed with the `<no>` value, Kaspersky Endpoint Agent will not analyze data on files. If the IOC file contains the terms of the FileItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only analyze data on files if the FileItem IOC document is described in the IOC file submitted for scanning.

--network=no	Optional parameter. This parameter enables threat lookup based on the Network IOC document during IOC scanning. If the <no> value is set for the parameter, Kaspersky Endpoint Agent does not perform threat lookup based on the Network IOC document. If the IOC file contains the terms of the Network IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent only enables threat lookup based on the Network IOC document if the Network IOC document is described in the IOC file submitted for scanning.
--url=no	Optional parameter. This parameter enables threat lookup based on the UrlHistoryItem IOC document during IOC Scanning. If the <no> value is set for the parameter, Kaspersky Endpoint Agent will not perform threat lookup based on the UrlHistoryItem IOC document. If the IOC file contains the terms of the UrlHistoryItem IOC document, they will be ignored (defined as no match). If the parameter is not passed, Kaspersky Endpoint Agent will only enable threat lookup based on the UrlHistoryItem IOC document if the UrlHistoryItem IOC document is described in the IOC file submitted for scanning.
`--drives=<all|system|critical|custom>`	Optional parameter. This parameter allows you to specify the scope of the IOC scan when analyzing data for the FileItem IOC document. This parameter can have one of the following values: • `<all>` – the application scans all available file areas. • `<system>` – the application only scans files that are located in the folders where the operating system is installed. • `<critical>` – the application only scans temporary files that are located in user and system folders. • `<custom>` – the application only scans files that are located in the areas specified by the user. If the parameter is not passed, critical areas will be scanned.
`--Excludes=< list of exclusions >`	Optional parameter. This 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. If the parameter is not passed, all folders will be scanned, with no exclusions.
`--scope=< configurable list of folders >`	Optional parameter. This parameter becomes required if the `--drives=custom` parameter is passed. This parameter allows you to specify a list of scan areas. Several values separated by space can be passed by the parameter.
`--retro`	Optional parameter. The parameter is used to start the task in the **Retrospective IOC scan** mode. In addition to this parameter, you can specify the time interval within which the application will perform a retrospective IOC scan using the following parameters: • `--start-time=< interval start date and time >` • `--end-time=< interval end date and time >` Example: `agent.exe --scan-ioc --path=<path to the folder with IOC files> --retro --start-time=2021-05-21T10:30:00Z --end-time=2021-05-24T10:30:00Z` If the time interval is not specified, the default interval will be used, starting one day before the task was started and ending at the moment the task was launched.

Return codes of the `--scan-ioc` command:

- `-1` – command is not supported by Kaspersky Endpoint Agent version installed on the device.
- `0` – command successfully executed.
- `1` – required argument is not passed to the command.

- 2 – general error.
- 4 – syntax error.

If the command was executed successfully (code `0`) and indicators of compromise were detected during the 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 an 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 where a match was detected.
`Date`	Creation date of the file where indicators of compromise were detected.
`Created`	Only for FileItem. Creation time of the object where indicators of compromise were detected.
`Pid`	Identifier of the process for which indicators of compromise were detected.
`Upid`	Unique identifier of the process for which indicators of compromise were detected.
`ParentPid`	Identifier of the parent object that contains the process for which indicators of compromise were detected.
`Username`	Name of the user who made changes to the object being scanned.
`StartTime`	Start time of the process for which indicators of compromise were detected.

Managing scanning of files and processes according to YARA rules

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

YARA scanning is a process that you can create and configure manually using the command line interface. YARA files are used to run the scan.

Only the files with YARA rules can be specified for the YARA Scan task. Files with other types of rules are not supported for the YARA Scan task.

To run a YARA scan using 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-yara [< path to the YARA file >] [--path=< path to the folder with YARA rules >] [--fast-scan] [--tag-hint=< tag rule >] [--id-hint=< rule ID >] [--max-rules= < maximum number of scan rules >] [--timeout=< stop scan after the specified time in seconds >] [--recursive] [--scan_folders [< list of folders to be scanned >] [--scan-memory] [--scan-process < process name >][--max-size=< file size in bytes >] [--excludes < list of objects to be scanned >] [--includes < list of objects to be scanned >]
```

If the `--scan-yara` command is passed with only the required parameters, Kaspersky Endpoint Agent will perform the scan with the default settings.

The scan parameters are described in the following table.

Command parameters when starting and configuring YARA scan

Parameters	Description
`--scan-yara [< full path to the YARA file >]`	Required parameter. Starts a YARA scan on the device. The scan is performed according to the rules in the YARA files with the yara or yar extension. Several values, separated by spaces, can be passed to the parameter. At least one `<full path to the yara file>` value must be specified if the --path parameter is not specified. If the --path parameter is also specified in addition to the arguments of the --scan-yara parameter, the scan uses both the files with the YARA rules specified as the arguments and the files from the folder specified by the --path parameter.
`--path=<path path to the folder with the YARA files >`	Path to the folder with the YARA files that you want to scan. Required parameter, if the `< full path to the YARA file >` parameter is not specified.
`--fast-scan`	Optional parameter. The parameter starts the fast scan mode. For each scan object, one occurrence of the detected marker is logged, and duplicates of the detected markers are not logged. Usage of this parameter allows you to reduce the time for scanning large files. If the parameter is not passed, a standard scan is performed and the duplicates of detected markers are logged.
`--tag-hint=< tag rule >`	Optional parameter. The parameter allows considering only the rules with the specified tag during scan. You can specify only one parameter value. Rules without tags or with tags other than those specified as the parameter value are ignored during scan. If the parameter is not passed, all the rules are considered during scan.
`--id-hint=<rule rule ID >`	Optional parameter. The parameter allows considering only the rules with the specified ID during scan. You can specify only one parameter value. Rules without IDs or with IDs other than those specified as the parameter value are ignored during scan. If the parameter is not passed, all the rules are considered during scan.
`--max-rules=< maximum number of scan rules >`	Optional parameter. The parameter sets the limit of unique triggered detection rules; scan stops upon exceeding this limit. If the parameter value is not specified or equals to 0, the scan is performed without limitations.
`--timeout=< stop scan after the specified time in seconds >`	Optional parameter. The parameter specifies the scan duration in seconds. The scan will be stopped after the specified time. If the parameter value is not specified or equals to 0, the scan is performed without limitations.
`--recursive`	Optional parameter. The parameter starts recursive scan of subfolders within the [<list of folders to be scanned>] value.

`--scan_folders [<list of folders to be scanned>]`	Optional parameter. This parameter starts a scan of the files in the specified list of folders. If the value of the <`list of folders to be scanned`> parameter is not specified, the scan is performed recursively for all local drives, except for network, cloud, and connected drives.
`--scan-memory`	Optional parameter. This parameter starts a memory scan for all running processes.
`--scan-process <process name>`	Optional parameter. This parameter starts a memory scan for only specified processes. Standard masks are supported for the <`process name`> value: "`?`" and "`*`".
`--max-size=<file size in bytes>`	Optional parameter. Scan is performed only for the files that do not exceed the specified size. Larger files are skipped during scan.
`--includes <list of objects to be scanned>`	Optional parameter. This parameter allows you to limit the scan scope. You can specify several parameter values separated by a space. Available values: • File name • File path • File name mask • File path mask Passed with the --scan-folders parameter. Example: --scan-folders c:*.* --recursive --includes *.exe c:\temp*.* *.dll – the scan will be performed for all files with the "exe" and "dll" extensions on the C: drive, and all files in the c:\temp folder will be scanned recursively.
`--excludes <list of objects to be scanned>`	Optional parameter. This parameter excludes the specified files or folders from the scan. You can specify several parameter values separated by a space. Available values: • File name • File path • File name mask • File path mask Passed with the --scan-folders parameter. Example: --scan-folders c:*.* --excludes readme.txt c:\trusted*.* *.xml – the readme.txt files, all files from the c:\trusted folder, and all files with the xml extension in the root folder on the C: drive will be skipped during the scan.

Return codes of the `--scan-yara` command:

- `-1` – command is not supported by Kaspersky Endpoint Agent version installed on the device.
- `0` – command successfully executed.
- `1` – required argument is not passed to the command.
- `2` – general error.
- `4` – syntax error.
- `5` – one or more files with YARA rules specified as the parameter value not found.

If the command execution completed successfully (code `0`) and indicators of compromise were detected during the command execution, Kaspersky Endpoint Agent displays the scan results in the command line. The scan results are described in the following table:

Data displayed by the application in the command line when YARA signatures are detected.

`Offset`	Offset in the object scanned by Kaspersky Endpoint Agent.
`Data`	Signatures searched by Kaspersky Endpoint Agent during scanning.
`Object Name`	The name of the scanned object.
`Rule Name`	The name of the rule used during scan.

Managing scanning of autorun point objects according to YARA rules

This Help provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

YARA scanning of the autorun points is a process that you can create and configure manually using the command line interface. YARA files are used to run the scan.

Only files with YARA rules can be specified in the YARA Scan task for autorun point objects. Files with other types of rules are not supported for the YARA Scan task.

By default, scanning of objects according to YARA rules is performed for the following types of autorun points:

- Logon
- Run
- Explorer
- Shell
- Office
- Internet Explorer
- Tasks
- Services
- Drivers
- Telephony
- Cryptography
- Debuggers
- COM
- Session Manager

- Network
- LSA
- Applications
- Codecs
- Shellex
- Unspecified

To run a YARA scan of autorun points using 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-yara [< path to the YARA file >] [--path=< path to the file with the YARA rules >] --scan-autoruns=yes [--fast-scan] [--tag-hint=< rule tag >] [--id-hint=< rule ID >] [--max-rules=< maximum number of scan rules >] [--timeout=< stop scan after the specified time in seconds >] [--max-size=< file size in bytes >] [--exclude-autoruns=COM]`

   If the `--scan-yara --scan-autoruns` command is passed with only the required parameters, Kaspersky Endpoint Agent performs a scan with the default settings.

The scan parameters are described in the following table.

Command parameters when starting and configuring YARA scan

Parameters	Description
`--scan-yara [< full path to the YARA file >]`	Required parameter. Starts a YARA scan for the autorun point files on the device. The scan is performed according to the rules in YARA files with the yara or yar extension. Several values separated by spaces can be passed to the parameter. At least one `<full path to the yara file>` value must be specified if the --path parameter is not specified. If the `--path` parameter is also specified in addition to the arguments of the `--scan-yara --scan-autoruns` parameter, the scan uses both the files with the YARA rules specified as the arguments and the files from the folder specified by the `--path` parameter.
`--path=<path path to the folder with the YARA files >`	Path to the folder with the YARA files that you want to use to search for autorun point files. Required parameter, if the `< full path the YARA file >` parameter is not specified.
`--scan-autoruns=yes`	Required parameter. This parameter accesses autorun points and scans objects for all types of autorun points according to the specified YARA rules. Specify the `yes` value to start the scan. If parameter value is not specified, the parameter will be ignored.

`--fast-scan`	Optional parameter. The parameter starts the fast scan mode. For each scan object, one occurrence of the detected marker is logged, and duplicates of the detected markers are not logged. Usage of this parameter allows you to reduce the time for scanning large files. If the parameter is not passed, a standard scan will be performed and the duplicates of detected markers will be logged.
`--tag-hint=< tag rule >`	Optional parameter. The parameter allows considering only the rules with the specified tag during scan. You can specify only one parameter value. Rules without tags or with tags other than those specified as the parameter value are ignored during scan. If the parameter is not passed, all the rules are considered during scan.
`--id-hint=<rule rule ID >`	Optional parameter. The parameter allows considering only the rules with the specified ID during scan. You can specify only one parameter value. Rules without IDs or with IDs other than those specified as the parameter value are ignored during scan. If the parameter is not passed, all the rules are considered during scan.
`--max-rules=< maximum number of scan rules >`	Optional parameter. This parameter sets the limit of unique triggered detection rules; the scan will stop upon exceeding this limit. If the parameter value is not specified or equals 0, the scan will be performed without limitations.
`--timeout=< stop scan after the specified time in seconds >`	Optional parameter. This parameter specifies the scan duration of each object in seconds. The scan will be stopped after the specified time. If the parameter value is not specified or equals to 0, the scan is performed without limitations.
`--max-size=< file size in bytes> >`	Optional parameter. Scan is performed only for the files that do not exceed the specified size. Larger files are skipped during scan.
`--exclude-autoruns=< list of objects to be scanned >`	Optional parameter. This parameter excludes files of the specified autorun point from the scan. You can specify several parameter values separated by a space. Available value: COM (as of this writing, only this type of autorun point can be excluded from a scan). Example: `--exclude-autoruns=COM` The files from the COM autorun point scope will be ignored during the scan. **Limitations** The resulting lists of autorun points for COM objects may not contain component builds developed using .NET due to the special aspects of their registration in the system.

Return codes of the `--scan-yara` command:

- `-1` – command is not supported by Kaspersky Endpoint Agent version installed on the device.
- `0` – command successfully executed.
- `1` – required argument is not passed to the command.
- `2` – general error.
- `4` – syntax error.
- `5` – one or more files with YARA rules specified as the parameter value not found.

If the command execution completed successfully (code `0`) and indicators of compromise were detected during the command execution, Kaspersky Endpoint Agent displays the scan results in the command line. The scan results are described in the following table:

Data displayed by the application in the command line when YARA signatures are detected.

`Offset`	Offset in the object scanned by Kaspersky Endpoint Agent.
`Data`	Signatures searched by Kaspersky Endpoint Agent during scanning.
`Object Name`	The name of the scanned object.
`Rule Name`	The name of the rule used during scan.

Creating a memory dump

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can create a memory dump for the computer on which Kaspersky Endpoint Agent is installed.

Before creating the memory dump, we recommend terminating processes of critical applications. After creating the memory dump, we recommend restarting the computer for which the memory dump was created.

To create a memory dump using the Kaspersky Endpoint Agent 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, enter the command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

3. Enter the command:

   `agent.exe --memory-dump --path=<path to local or network folder where you want to save the memory dump> [--user=<user name> --pwd=<password>]`.

   The user name and password are required if a folder for storing the memory dump is password protected.

   Be sure that write access is granted for the folder where the memory dump will be stored. Otherwise, dump file will not be created.

4. Press **ENTER**.

   In the specified folder, Kaspersky Endpoint Agent creates a memory dump with the name MemoryDump_<host name>_<date and time when the file began to be written>.dmp.

Command parameters for creating a memory dump

Parameter	Description
`--path`	Required parameter. This parameter passes the full path to the local or network folder where the application will store the memory dump. The name of a network folder must be in UNC format.
`--user`	This parameter passes the user name for accessing the folder specified by the `--path` parameter. If this parameter is missing, the SYSTEM account must have access to the folder.
`--pwd`	This parameter passes the password for accessing the folder specified by the `--path` parameter. If this parameter is missing, the SYSTEM account must have access to the folder.

Return codes of the `--memory-dump` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

Kaspersky Endpoint Agent does not encrypt or compress the memory dump file. If necessary, you can use third-party tools to encrypt and compress of the folder where the memory dump is stored.

The SMB 3 (or higher) protocol must be configured in order for Kaspersky Endpoint Agent to save the memory dump file to the folder in encrypted form.

Creating a disk dump

This section provides information related to Kaspersky Endpoint Agent for Windows. This information may be partially or completely inapplicable to Kaspersky Endpoint Agent for Linux. For complete information about Kaspersky Endpoint Agent for Linux, please refer to the Help of the solution that includes the application: Kaspersky Anti Targeted Attack Platform or Kaspersky Managed Detection and Response.

You can create a dump of a physical or logical disk of the computer on which Kaspersky Endpoint Agent is installed.

To create a disk dump using the Kaspersky Endpoint Agent 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, enter the command `cd "C:\Program Files (x86)\Kaspersky Lab\Endpoint Agent\"` and press **ENTER**.

   Enter the command:

```
agent.exe --disk-image --volume=<disk name> [--format=<file format, RAW or EWF>] [--max-size=<size in bytes>] [--segment-size=<size in bytes>] --path=<path to a local or network folder where you want to save the disk dump> [--user=<user name> --pwd=<password>]
```

The user name and password are required if the folder for storing the disk dump is password protected.

> Be sure that write access is granted for the folder where the disk dump will be stored. Otherwise, dump file will not be created.

3. Press **ENTER**.

In the specified folder, Kaspersky Endpoint Agent creates a disk dump file with a name in the format <disk name>_<date and time when the file started to be written>.<extension>.

The disk dump file extension may be the following:

- If the RAW format was specified in the command to create the disk dump (`--format=RAW`):
  - if the disk dump is not split (the `--segment-size` parameter is omitted), then the disk dump file has the raw extension;
  - If the disk dump is split (the `--segment-size` parameter is specified), then the parts of the dump have the extensions 001, 002, 003, etc. up to 999.
- If the EWF format was specified in the command to create the disk dump (`--format=EWF`):
  - If the disk dump is not split (the `--segment-size` parameter is omitted), then the disk dump file has the extension E01;
  - If the disk dump is split (the `--segment-size` parameter is specified), then the parts of the dump have the extension E01, E02, ..., E99; EAA, EAB, ..., EAZ; FAA, FAB, ..., FZZ, <...>; ZAA, ZAB, ..., ZZZ.

Command parameters for creating a disk dump

Parameter	Description
`--volume`	Required parameter. This parameter passes the number of a physical disk or the name of a logical disk, where the dump will be created. The format for the physical disk number is: \??\PHYSICALDRIVEN or PHYSICALDRIVEN, where N is the disk number. For example: \??\PHYSICALDRIVE0, PHYSICALDRIVE1. Format of the name of the logical disk: N:, where N is the letter designation of the logical disk. For example, C:. If you create a dump file for a logical disk used to boot the operating system, use the %SystemDrive% variable as the disk name.
`--format`	This parameter passes the format for the file with the disk dump. Possible values: RAW or EWF. If the parameter is omitted, the application creates a disk dump in the RAW format.
`--max-size`	This parameter passes the maximum allowed size of the disk dump in bytes. If this parameter is omitted, the application creates a disk dump with a maximum size of 1,099,511,627,776 bytes.
`--segment-size`	This parameter passes the maximum size of part of the disk dump in bytes. Additionally, the minimum size of part of the dump must be larger than 33,554,432 bytes. If the parameter is specified, the application splits the disk dump into parts of the specified size and adds them to an archive. The size of the archived dump parts is less than the value specified using the parameter. If the parameter is omitted, the application does not split the disk dump into parts.
`--path`	Required parameter. This parameter passes the full path to the local or network folder where the application stores the disk dump. The name of a network folder must be in UNC format.

Parameter	Description
`--user`	This parameter passes the user name for accessing the folder specified by the `--path` parameter. If the parameter is omitted, the SYSTEM access must have access to the folder where the disk dump will be stored.
`--pwd`	This parameter passes the password for accessing the folder specified by the `--path` parameter. If the parameter is omitted, the SYSTEM access must have access to the folder where the disk dump will be stored.

Return codes of the `--memory-dump` command:

- -1 – command is not supported.
- 0 – command successfully executed.
- 1 – required argument is not passed to the command.
- 2 – general error.
- 4 – syntax error.

Kaspersky Endpoint Agent does not encrypt or compress the memory dump file. If necessary, you can use third-party tools to encrypt and compress of the folder where the memory dump is stored.

The SMB 3 (or higher) protocol must be configured in order for Kaspersky Endpoint Agent to save the memory dump file to the folder in encrypted form.

Managing Kaspersky Endpoint Agent for Linux

This section provides information about Kaspersky Endpoint Agent for Linux. For information about Kaspersky Endpoint Agent for Windows, see a separate section.

Kaspersky Endpoint Agent for Linux is installed on individual devices running one of the supported Linux operating systems within the corporate IT infrastructure. The Application continuously monitors processes running on those devices, active network connections, and files that are being modified.

Kaspersky Endpoint Agent for Linux enables the interaction of the protected device with other Kaspersky solutions for complex threat detection (such as targeted attacks).

The program interacts with the Kaspersky Anti Targeted Attack Platform using the KATA Central Node component. When the integration of Kaspersky Endpoint Agent with KATA Central Node is configured, the program runs tasks and applies settings coming from KATA Central Node sends telemetry from the protected device to the KATA Central Node server.

You can remotely manage Kaspersky Endpoint Agent for Linux using the Kaspersky Security Center Web Console, the Kaspersky Security Center Administration Console, or the command line.

Installing and removing Kaspersky Endpoint Agent for Linux

This section provides information about installing Kaspersky Endpoint Agent for Linux on a device, updating the previous version of the application, restoring and removing the application from the device.

Preparing to install Kaspersky Endpoint Agent for Linux

Before installing Kaspersky Endpoint Agent for Linux on a device or updating the previous version of the application, you must verify that the device satisfies the hardware and software requirements.

Installing Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Administration Console

This section describes the remote installation of Kaspersky Endpoint Agent on a local device using Kaspersky Security Center Administration Console.

Installing the Kaspersky Endpoint Agent for Linux administration plug-in

You can manage Kaspersky Endpoint Agent in the Kaspersky Security Console by using the administration plug-in. Therefore, to gain access to the program management interface, the administration plug-in must be installed on the administrator's workstation.

To install the Kaspersky Endpoint Agent administration plug-in,

copy the klcfginst.msi file from the distribution kit to the device where Kaspersky Security Center Administration Console is installed and run the file.

The Setup Wizard of the program starts.

Adding devices for installing Kaspersky Endpoint Agent for Linux

To install the program remotely using Kaspersky Security Center, you must add the devices that you are installing the program on to the managed devices group.

To add devices for installing the application:

1. Install the Kaspersky Security Center Network Agent on the device.

   The procedure for preparing a Linux-running device for remote installation of Network Agent is described in the *Kaspersky Security Center Help*.

2. In the command line, run the following command: `/opt/kaspersky/klnagent/bin/klmover --address <IP address of the Kaspersky Security Center server>`.

   The device becomes available for management using Kaspersky Security Center.

   > If Network Agent was previously installed on the device, the first two steps of these instructions are not necessary.

3. Open the Kaspersky Security Center Administration Console.

4. In the console tree, select the **Managed devices** folder.

   > If Kaspersky Endpoint Security for Linux is installed on a device, the device will reside in the group in which the Kaspersky Endpoint Security for Linux policy is active. You do not need to move the device.

5. In the workspace of the folder, select the **Devices** tab.

6. Click **Move devices to group**.

   This opens the move devices wizard.

7. Click **Select devices discovered on the network by the Administration Server**.

8. In the next window of the wizard, in the list of devices, select the check box next to the device where you need to install the program.

9. Click **Next**.

   The device is moved to the managed devices group.

10. Click **Finish** to complete the wizard.

The device will become available for remote installation of the application.

Creating an installation package for Kaspersky Endpoint Agent for Linux

To remotely install the program using Kaspersky Security Center, you must create an installation package for Kaspersky Endpoint Agent from the Kaspersky repository or from a file.

> Before creating the Kaspersky Endpoint Agent installation package, make sure that the administration plug-in is installed on the administrator workstation.

To create an installation package for the program from the Kaspersky program repository:

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, in the **Administration Server** → **Advanced** → **Remote installation** folder, select the **Installation packages** subfolder.
3. Click **Create an installation package** to start the installation package creation wizard.
4. In the **Select installation package type** window of the wizard, click **Create an installation package for a Kaspersky application**.

   When creating an installation package for a program, you will be prompted to read the End User License Agreement for that program and the Privacy Policy of that program. Carefully read the End User License Agreement between you and Kaspersky Lab, as well as the Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm that I have fully read, understand, and accept** section:

   - **The terms and conditions of this End User License Agreement**
   - **Privacy Policy describing the handling of data**
5. In the next window of the wizard, enter the name for the new installation package.
6. In the next window of the wizard, select the Kaspersky Endpoint Agent installation file with the "kud" extension.
7. In the next window of the wizard, select Kaspersky Endpoint Agent components that you need to install, the installation directory and the installation mode of the program.

After the wizard finishes, the created installation package appears in the workspace of the **Installation packages** folder in the console tree.

To create an installation package for the program from a file:

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, in the **Administration Server** → **Advanced** → **Remote installation** folder, select the **Installation packages** subfolder.

3. Click **Create an installation package** to start the installation package creation wizard.

4. In the **Select installation package type** window of the wizard, click **Create an installation package for the specified executable file**.

   When creating an installation package for a program, you will be prompted to read the End User License Agreement for that program and the Privacy Policy of that program. Carefully read the End User License Agreement between you and Kaspersky Lab, as well as the Privacy Policy. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm that I have fully read, understand, and accept** section:

   - **The terms and conditions of this End User License Agreement**
   - **Privacy Policy describing the handling of data**

5. In the next window of the wizard, enter a name for the installation package.

6. In the next window of the wizard, select the installation file of the program and complete the creation of the installation package by following the directions of the wizard.

After the wizard finishes, the created installation package appears in the workspace of the **Installation packages** folder in the console tree.

Remote installation of Kaspersky Endpoint Agent for Linux on selected devices

Kaspersky Security Center allows you to install applications on devices remotely, using remote installation tasks.

To create and run the task to remotely install Kaspersky Endpoint Agent on selected devices:

1. Open the Kaspersky Security Center Administration Console.

2. In the console tree, in the **Remote installation** folder, select the **Installation packages** subfolder.

3. In the workspace of the folder, select the installation package of Kaspersky Endpoint Agent.

4. In the context menu of the installation package, select **Install program**.

5. The Remote Installation Wizard starts.

6. In the **Select devices for installation**, you can create a list of devices to install the program on.

7. In the **Configure the remote installation task**, configure the remote installation of the program.

8. In the **Select operating system reboot option** window, select whether the devices will be rebooted if a system reboot is required during installation.

9. In the **Select accounts for access to devices** window, you can add accounts that will be used to start the remote installation task.

10. In the **Start installation** window, click **Next** to create and start the remote installation task on selected devices.

    If in the **Start installation** window, the **Do not start the task after the remote installation wizard finishes** check box is selected, the remote installation task is not started. You can start this task manually later. The name of the task corresponds to the name of the installation package for installing the program: **Install <name of the installation package>**.

Installing Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console

This section describes the remote installation of Kaspersky Endpoint Agent for Linux on a local device using Kaspersky Security Center Web Console.

Installing the Kaspersky Endpoint Agent web administration plug-in

You can manage Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console with the web administration plug-in. Therefore to gain access to program management, you must install the web administration plug-in on the administrator workstation (see information on installing and updating the web administration plug-in in the help section that describes the management of Kaspersky Endpoint Agent for Windows).

Before installing, familiarize yourself with the information about compatible versions of the web administration plug-in.

Adding devices for installing Kaspersky Endpoint Agent for Linux

To install the program remotely using Kaspersky Security Center, you must add the devices that you are installing the program on to the managed devices group.

To add devices for installing the application:

1. Install the Kaspersky Security Center Network Agent on the device.

   The procedure for preparing a Linux-running device for remote installation of Network Agent is described in the *Kaspersky Security Center Help*.

2. In the command line, run the following command: `/opt/kaspersky/klnagent/bin/klmover --address <IP address of the Kaspersky Security Center server>`.

   The device becomes available for management using Kaspersky Security Center.

   > If Network Agent was previously installed on the device, the first two steps of these instructions are not necessary.

3. Log in to the Kaspersky Security Center Web Console.

4. In the main window of the web console, select **Device discovery** -> **Unassigned devices**.

   > If Kaspersky Endpoint Security for Linux is installed on a device, the device will reside in the group in which the Kaspersky Endpoint Security for Linux policy is active. You do not need to move the device.

5. In the list of devices, select the check box next to the device where you need to install the application.

6. Click **Move to group**.

7. This opens a menu on the right side; in the menu, select the check box next to the **Managed devices** group.

8. Click **Move**.

The device will become available for remote installation of the application.

Creating an installation package for Kaspersky Endpoint Agent for Linux

To remotely install the program using Kaspersky Security Center Web Console, you must create an installation package for Kaspersky Endpoint Agent for Linux from the Kaspersky program repository or from a file.

To create an installation package for the program:

1. Log in to the Kaspersky Security Center Web Console.

2. On the **Discovery & Deployment** tab, select **Deployment & Assignment** → **Installation packages**.

3. Click **Add**.

   This starts the New Package Wizard. To continue with the wizard, click **Next**.

4. At the first step of the wizard, you can select how you want to create the installation package: from the Kaspersky program repository or from a file.

   - If you selected **Create an installation package for a Kaspersky application**, a list of installation packages available on Kaspersky web servers is displayed. To make finding the necessary installation package easier, click **Filter**, and in the menu that opens in the **Property** window, select **Operating system** and the **Linux** option.

   - If you selected **Create an installation package from a file**, you are prompted to enter the path to a local folder containing the archive with the installation package of the program.

5. Select the necessary Kaspersky Endpoint Agent for Linux installation package.

   This opens a window containing information about the installation package.

6. Read the information and click **Download and create installation package**.

   The installation package begins downloading to the Administration Server.

7. While the download is in progress, the **Accept** button is displayed. Do the following:

   a. Click **Accept** to read the text of the License Agreement and the Privacy Policy.

   b. If you agree with all the terms of the License Agreement and the Privacy Policy, select the following check boxes in the **I confirm that I have fully read, understand, and accept** section:

      - **the terms and conditions of this End User License Agreement**

      - **Privacy Policy describing the handling of data**

c. Click **Accept**.

The download of the installation package resumes after both check boxes are selected. If you click **Decline**, the download is canceled.

8. After the download is complete, click **Close** to close the installation package information window.

The downloaded installation package is located in the Packages subfolder within the shared folder of the Administration Server. The downloaded installation package is displayed in the list of installation packages.

Remote installation of Kaspersky Endpoint Agent for Linux on selected devices

Kaspersky Security Center Web Console allows you to install applications on devices remotely, using remote installation tasks.

To create and run the task to remotely install Kaspersky Endpoint Agent for Linux on selected devices:

1. Log in to the Kaspersky Security Center Web Console.
2. On the **Devices** tab, select **Tasks**.
3. Click **Add**.

   The New Task Wizard starts. Follow the instructions of the wizard.
4. At the first step of the wizard:

   a. In the **Application** window, select **Kaspersky Security Center 12**.

   b. In the **Task type** window, select **Install application remotely** as the task type.

   c. If necessary, enter a name for the task in the **Task name** window.

   d. In the **Select devices to which the task will be assigned** section, select **Device group**.
5. Click **Next**.

   This opens the next screen of the New Task Wizard.
6. Select the check box next to the **Managed devices** group or check boxes next to individual devices in that group.
7. Click **Next**.

   This opens the next screen of the New Task Wizard.
8. In the **Selecting installation package** window, select the Kaspersky Endpoint Agent for Linux that you created earlier.

   Do not modify any other options at this step or the subsequent steps.
9. Click **Next**.

   This opens the final step of the New Task Wizard.
10. At the final step of the Wizard, click **Finish**.

11. Select the check box next to the created task in the task list.
12. Click **Start**.
13. Wait until the installation of Kaspersky Endpoint Agent for Linux on selected devices is complete.

    The status of the task changes to **Completed**.

Local installation of Kaspersky Endpoint Agent for Linux

This section contains information about installing Kaspersky Endpoint Agent on a local device from DEB or RPM installation packages.

To install the program or update an older version of the program:

1. Copy the DEB or RPM installation package of the program from the distribution kit to the user device.
2. Open the console and run the command to install the program from the relevant package:
   - To install the program from a deb installation package: `sudo apt install package_name.deb`
   - To install the program from an rpm installation package: `sudo rpm -i package_name.rpm`

   The program is installed on the local device.

To use the program, you must accept the terms and conditions of the End User License Agreement and the Privacy Policy.

Too view the End User License Agreement and the Privacy Policy and accept the terms and conditions:

1. Open the console and run the `/opt/kaspersky/epagent/sbin/lenactl --eula-pp accept` command.
2. Carefully read the End User License Agreement between you and Kaspersky Lab.
3. Click **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement**.
4. Carefully read the terms and conditions of the Privacy Policy.
5. Click **I understand and agree that my information will be processed and transmitted (including to third countries) in accordance with the Privacy Policy. I confirm that I have fully read and understand the Privacy Policy**.

   The program is ready for use.

Updating and restoring Kaspersky Endpoint Agent for Linux

The program can be updated and restored using Kaspersky Security Center or locally.

To update Kaspersky Endpoint Agent for Linux using Kaspersky Security Center, you must create an installation package for the new version and follow the installation procedure. To restore the application, you can use the installation package created for the current version of the application.

Removing Kaspersky Endpoint Agent for Linux

The program can be removed using Kaspersky Security Center or locally.

To remove the program remotely from selected devices using Kaspersky Security Center:

1. Log in to the Kaspersky Security Center Web Console.
2. On the **Devices** tab, select **Tasks**.
3. Click **Add**.

   Follow the instructions of the New Task Wizard.
4. At the first step of the wizard:
   a. In the **Application** window, select **Kaspersky Security Center 12**.
   b. In the **Task type** window, select **Uninstall application remotely** as the task type.
   c. If necessary, enter a name for the task in the **Task name** window.
   d. In the **Select devices to which the task will be assigned** section, select **Device group**.
5. Click **Next**.

   This opens the next screen of the New Task Wizard.
6. Select the check box next to the **Managed devices** group or check boxes next to individual devices in that group.
7. Click **Next**.

   This opens the next screen of the New Task Wizard.
8. In the **Application to uninstall** window, select the installed version of Kaspersky Endpoint Agent for Linux.

   Do not modify any other options at this step or the subsequent steps.
9. At the last step of the Wizard, click **Finish**.
10. Select the check box next to the created task in the task list and click **Start**.
11. Wait until the removal of Kaspersky Endpoint Agent for Linux from the selected devices is complete.

    The task status changes to **Completed**.

Upon completion of the task, the selected application is removed from the selected devices.

Managing Kaspersky Endpoint Agent for Linux policies using Kaspersky Security Center Administration Console

Kaspersky Security Center is designed for centralized running of basic administration and maintenance tasks for an organization's network security system. The application provides the administrator with access to detailed information about the organization's network security level; it lets you configure all the components of protection based on Kaspersky Lab applications.

You can use Kaspersky Security Center to remotely install and remove Kaspersky Endpoint Agent and configure the operation of the program.

For detailed information about Kaspersky Security Center, please refer to the *Kaspersky Security Center Help*.

The user interface for working with Kaspersky Security Center is provided by the Kaspersky Security Center Administration Console.

You can manage Kaspersky Endpoint Agent using Kaspersky Security Center Web Console with the *Kaspersky Endpoint Agent administration plug-in*.

The following information in this section describes how to manage Kaspersky Endpoint Agent using the Kaspersky Security Center Administration Console.

Managing policies of Kaspersky Endpoint Agent for Linux

This section provides instructions for creating a policy for Kaspersky Endpoint Agent for Linux and enabling options in the policy using Kaspersky Security Center Administration Console.

Instructions in this section apply only to Kaspersky Endpoint Agent for Linux. For information about Kaspersky Endpoint Agent for Windows, see a separate section.

Creating a policy for Kaspersky Endpoint Agent for Linux

To create a policy for Kaspersky Endpoint Agent in Kaspersky Security Center:

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Click **Create policy**.

   The New Policy Wizard starts.
4. In the **Enter group policy name**, window, enter the name that will be used to display the new policy in the list of policies.

5. In the **Select policy type**, select a Kaspersky Endpoint Agent deployment mode by selecting the **Endpoint Detection and Response Expert (KATA EDR)** check box.

6. Click **Next**.

7. Do one of the following in all settings windows that are displayed in sequence:

   - To configure program settings from the displayed sections when creating the policy:

     a. Click **Configure** next to the name of the section.

     b. This opens a window; in that window, modify the relevant settings and click **OK.**

     c. Click **Next**.

   - To configure the displayed sections later, click **Next**.

   Program configuration involves the following steps:

   - Configuring general proxy server settings.
   - Configuring the integration of Kaspersky Endpoint Agent with KATA Central Node.

8. In the **Target group** window, select the Kaspersky Security Center administration group that the new policy must affect:

   a. Click **Browse**.

   This opens the administration group selection window.

   b. Select an administration group from the list.

   For example, you can select the **Managed devices** group.

   c. If you want to create a device subgroup in the **Managed devices** group:

      1. Click **New group**.

      2. This opens a window; in that window, enter the name of the device subgroup.

      3. Click **OK**.

   d. Click **Next**.

9. In the **Create group policy for the program** select one of the following policy states:

   - **Active policy** to activate the policy immediately after creation.
   - **Inactive policy** to activate the policy later.

10. Select the **Open policy properties immediately after creation** if you need to perform additional configuration of the policy right after it is created.

11. Click **Finish**.

The policy that you created appears in the list of politics.

Enabling options in the policy of Kaspersky Endpoint Agent for Linux

When configuring default settings of a Kaspersky Endpoint Agent policy, setting values are saved but not applied until you enable them.

You can enable settings by enabling groups in which the settings reside. In one policy you can enable some groups of settings or all groups of settings.

To enable a group of settings in the Kaspersky Endpoint Agent policy:

1. Open the Kaspersky Security Center Administration Console.
2. In the console tree, open the **Policies** folder.
3. Select a policy for Kaspersky Endpoint Agent and open its settings window in one of the following ways:
   - Double-click on the name of the policy.
   - In the context menu of the policy, select **Properties**.
4. In the opened window, select the **Application settings** tab.
   a. Select the **Other settings** subsection.
   b. Select one of the following options for using a proxy server:
      - **Do not use proxy server**.
      - **Use proxy server with specified settings**.

      If you selected **Use proxy server with specified settings**, in the **Server name or IP address** and **Port**, enter the address and port of the proxy server to which you want to connect. Port 8080 is used by default.

      Kaspersky Endpoint Agent does not encrypt the connection with the proxy server. You must take steps to make sure the network connection between your proxy server and Kaspersky Endpoint Agent is secure.

      If you want to use NTLM authentication when connecting to the proxy server:

      1. Select the **Use NTLM authentication by user name and password**.
      2. In the **User name** field, enter the name of the user whose account will be used for authorization at the proxy server.
      3. In the **Password** field, enter the password to obtain connection to the proxy server.

      To reveal password characters, click **Show** to the right of the **Password** field.

      If you do not want to use the proxy server for addresses internal to the organization, select the **Bypass proxy server for local addresses** check box.

   c. Click **Apply**.

5. Select the **KATA integration** section.

   a. Go to the **General Settings** subsection.

   b. In the **Data transmission settings** group, set the **Under policy** toggle switch to active.

   c. In the **Event transmission period (sec.)** field, type 30.

   d. In the **Event limit per one package**, type 1024.

   e. In the **Throttling settings** group, set the **Under policy** toggle switch to active.

   f. Select the **Enable throttling** check box.

   g. Enter the maximum number of events per hour and the percentage value for events exceeding the limit.

   h. Go to the **KATA integration settings** subsection.

   i. In the **Connection settings** group, move the **Enforce** toggle switch to active.

   j. Select the **Enable KATA integration** check box.

   k. Enter the address and port of the KATA server in the **Address** and **Port** fields.

   l. Select the **Use pinned certificate to secure connection** check box.

   m. Click **Add new TLS certificate**.

   n. In the opened window, click **Upload** and select the server certificate file to set up a secure connection or enter certificate data in the field.

   o. Click **Add**.

   p. Click **Add client certificate**.

   q. In the opened window, select the **Secure with client certificate** check box.

   r. Click **Upload** and select a client certificate file to set up a secure connection.

   s. In the **Cryptographic container password** field, enter the password of the client certificate to set up a secure connection.

   t. Select the **Apply TTL period for events transmission**.

   u. In the **TTL period (min.)** field, enter the interval for sending synchronization requests.

   v. Click **Apply**.

6. Click **OK**.

Policy settings required by Kaspersky Endpoint Agent are enabled.

Managing database and module update tasks for Kaspersky Endpoint Agent

You can create and configure program database and module update tasks using Kaspersky Security Center Administration Console (see the help section describing how to create and configure program database and module update tasks in Kaspersky Endpoint Agent for Windows).

You can also configure program database and module updates using the command line.

Managing Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console

Kaspersky Security Center is designed for centralized running of basic administration and maintenance tasks for an organization's network security system. The application provides the administrator with access to detailed information about the organization's network security level; it lets you configure all the components of protection based on Kaspersky Lab applications.

You can use Kaspersky Security Center to remotely install and remove Kaspersky Endpoint Agent for Linux and configure the operation of the application.

For detailed information about Kaspersky Security Center, please refer to the *Kaspersky Security Center Help*.

The user interface for working with Kaspersky Security Center is provided by the Kaspersky Security Center Web Console component.

You can manage Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console with the *Kaspersky Endpoint Agent web administration plug-in*.

The following information in this section describes how to manage Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console.

Managing policies of Kaspersky Endpoint Agent for Linux

This section provides instructions for creating a policy for Kaspersky Endpoint Agent for Linux and enabling options in the policy using Kaspersky Security Center Web Console.

Instructions in this section apply only to Kaspersky Endpoint Agent for Linux. For information about Kaspersky Endpoint Agent for Windows, see a separate section.

Creating a policy for Kaspersky Endpoint Agent for Linux

To create a policy for Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console:

1. Log in to the Kaspersky Security Center Web Console.
2. On the **Devices** tab, select **Policies & Profiles**.
3. Click **Add**.

   Follow the instructions of the New Policy Wizard.
4. At the first step of the wizard, select **Kaspersky Endpoint Agent**.
5. Click **Next**.
6. Make sure the **Kaspersky Endpoint Detection and Response Expert (KATA EDR)** check box is selected.
7. Click **Next**.
8. At the last step of the Wizard, specify the new policy name, change the state of the policy (by default, the policy is *Active*), and configure the inheritance of settings.
9. Click **Save**.

The policy that you created appears in the list of politics.

Enabling options in the policy of Kaspersky Endpoint Agent for Linux

To enable settings in a policy for Kaspersky Endpoint Agent for Linux using Kaspersky Security Center Web Console:

1. Log in to the Kaspersky Security Center Web Console.
2. On the **Devices** tab, select **Policies & Profiles**.
3. Click a previously created **Kaspersky Endpoint Agent** policy.

   This opens the policy settings window.
4. Select the **Application settings** section.

   a. Select the **Other settings** subsection.

   b. Select one of the following options for using a proxy server:

   - **Do not use proxy server**.
   - **Use proxy server with specified settings**.

   If you selected **Use proxy server with specified settings**, in the **Server name or IP address** and **Port**, enter the address and port of the proxy server to which you want to connect. Port 8080 is used by default.

Kaspersky Endpoint Agent for Linux does not encrypt the connection with the proxy server. You must take steps to make sure the network connection between your proxy server and Kaspersky Endpoint Agent for Linux is secure.

If you want to use NTLM authentication when connecting to the proxy server:

1. Select the **Use NTLM authentication by user name and password**.
2. In the **User name** field, enter the name of the user whose account will be used for authorization at the proxy server.
3. In the **Password** field, enter the password to obtain connection to the proxy server.

To reveal password characters, click **Show** to the right of the **Password** field.

If you do not want to use the proxy server for addresses internal to the organization, select the **Bypass proxy server for local addresses** check box.

If you are configuring policy settings, in the upper right corner of the group of settings, move the toggle switch from **Undefined** to **Enforce**.

c. Click **OK**.

5. In the **KATA integration** section:

a. Go to the **General Settings** subsection.

b. In the **Data transmission settings** group, move the **Enforce** toggle switch to active.

c. In the **Event transmission period (sec.)** field, type 30.

d. In the **Event limit per one package**, type 1024.

e. In the **Throttling settings** group, select the **Enable throttling** check box.

f. Enter the maximum number of events per hour and the percentage value for events exceeding the limit.

g. Click **OK**.

h. Go to the **KATA integration settings** subsection.

i. In the **Connection settings** group, move the **Enforce** toggle switch to active.

j. Select the **Enable KATA integration** check box.

k. Enter the address and port of the KATA server in the **Server** and **Port** fields.

l. Select the **Use pinned certificate to secure connection** check box.

m. Click **Add new TLS certificate**.

n. In the opened tab, click **Upload** and select the server certificate file to set up a secure connection or enter certificate data in the **TLS certificate data** field.

o. Click **OK**.

p. In the **Additional security of the connection** group, select the **Secure with client certificate** check box.

q. Click **Upload cryptographic container** and select a client certificate file to set up a secure connection.

r. In the **Cryptographic container password** field, enter the password of the client certificate to set up a secure connection.

s. In the **Advanced** group:

a. In the **Send sync request to KATA server every (min.)** field, enter the synchronization interval in minutes.

b. Select the **Apply TTL period for events transmission**.

c. In the **TTL period (min.)** field, enter the interval for sending synchronization requests.

t. Click **OK**.

6. Click **Save**.

Policy settings required by Kaspersky Endpoint Agent for Linux are enabled.

Managing database and module update tasks for Kaspersky Endpoint Agent

You can also create and configure program database and module update tasks using Kaspersky Security Center Web Console (see the help section describing how to create and configure program database and module update tasks in Kaspersky Endpoint Agent for Windows).

You can also configure program database and module updates using the command line.

Managing Kaspersky Endpoint Agent for Linux using the command line

You can use the command line interface to run individual commands of Kaspersky Endpoint Agent for Linux.

The command line interface functionality is provided by the lenactl utility. This utility is included in the application distribution kit and is installed on each workstation in the /opt/kaspersky/epagent/sbin/ directory.

To run application commands through the command line interface:

1. Run the command line terminal on the device.
2. Enter the following command: `export PATH="$PATH:/opt/kaspersky/epagent/sbin/"`.
3. Press **ENTER**.

Now you can evoke the lenactl utility without specifying the path to the file.

4. Enter the command in the following format: `lenactl --param1 value`
5. Press **ENTER**.

   The command is executed.

The complete list of options and corresponding values is provided below.

Main commands of the program

`--product`

This option is used to run or stop the application and to display its current state.

Allowed values:

- `--product start` runs the unloaded program; this command runs the stopped service of the program
- `--product stop` stops the running program; this command stops the running service of the program
- `--product state` writes the current state of the program ("running" or "stopped") to the console

`--update`

This option updates program databases and modules once.

Allowed values and additional options:

- `--update` updates program databases from Kaspersky servers
- `--update <update_source>` updates program databases from the specified source
- `--update --app` updates databases and modules of the program from Kaspersky servers
- --update `<update_source> --app` updates databases and modules of the program from the specified source

`--local-update-task`

This option updates program databases and modules on a schedule using a local task.

> The local update task is created automatically when the program is run for the first time. By default, the task is in an inactive state. When an update task is created using Kaspersky Security Center, the local task is automatically and permanently deleted.

Allowed values and additional options:

- `--local-update-task enable-schedule` to enable hourly updates of program databases from Kaspersky servers.
- `--local-update-task --app enable-schedule` to enable hourly updates of program databases and modules from Kaspersky servers.
- `--local-update-task disable-schedule` to disable hourly updates of program databases from Kaspersky servers.
- `--local-update-task --app disable-schedule` to disable hourly updates of program databases and modules from Kaspersky servers.
- `--local-update-task <update_source>` to update program databases from the specified source.

`--proxy`

This option lets you use a proxy server.

> Kaspersky Endpoint Agent for Linux does not encrypt the connection with the proxy server. You must take steps to make sure the network connection between your proxy server and Kaspersky Endpoint Agent for Linux is secure.

Allowed values and additional options:

- `--server` — address of the proxy server
- `--port` — port of the proxy server
- `--user` — name of the proxy server user (optional)
- `--password` — password of the proxy server (if user name is specified)
- `--use-for-local` — use the proxy server for local addresses

`--traces`

This option is used to manage trace files of the application.

> All files in the trace file directory are considered to be trace files.

Allowed values and additional options:

- `--traces --on` turns on the trace file collection mode
- `--traces --off` turns off the trace file collection mode
- `--traces --clear` deletes all trace files in a directory
- `--traces --copyto <path to a directory>` copies trace files to the specified directory

> The systemd-journald system logging service can be active independently of the application and can maintain its own operation logs. This may slow down the interaction of the program with trace files and reduce available disk space.

To turn off audit logs of the systemd-journald system service:

1. `systemctl mask systemd-journald-audit.socket`
2. `systemctl restart systemd-journald`

`--help`

This option displays a command line option reference text.

Commands for configuring the interaction of the program with the EDR server

`--servers`

This option lets you specify the address and port of the EDR server.

The arguments can be represented by a semicolon-separated list of server:port pairs. Multiple server:port pairs can be passed to the input, however the program ignores all pairs except the first in the list.

Default value: none.

`--timeout`

This option lets you specify the timeout of the connection to the EDR server in milliseconds.

The argument can be represented by a number.

Default value: 100000.

`--sync-period`

This option lets you specify the synchronization period with the EDR server in seconds.

The argument can be represented by a number; the allowed range is 5-3600.

Default value: 300.

`--send-packet-period`

This option lets you specify the frequency with which telemetry packets are sent.

Argument: number; allowed range: 5-999.

Default value: 30

`--max-events-per-packet`

This option lets you specify the maximum number of events in a telemetry packet.

Argument: number; allowed range: 5-10000

Default value: 1024.

`--compression`

This option lets you apply compression.

Arguments: `<yes|no>`.

Default value: `no`.

`--tls`

This option lets you apply TLS encryption.

Arguments: `<yes|no>`.

Default value: `no`.

`--pinned-certificate`

This option lets you specify the path to the public part of the server certificate.

Argument: `<path to public part of server pinned certificate>`.

Default value: none.

`--client-certificate`

This option lets you specify the path to the container with the client certificate.

Argument: `<path to client certificate>`.

Default value: none.

`--client-password`

This option lets you specify the password of the container with the client certificate.

Argument: `<password>`.

Default value: none.

Verifying the integrity of Kaspersky Endpoint Agent for Linux components

To avoid the replacement of program manifest and files, Kaspersky Endpoint Agent can verify their integrity. The integrity verification utility verifies the integrity of files and modules listed in special lists that are called manifest files. A manifest file of a program component contains files and modules whose integrity is critical for correct operation of the component. The integrity of manifest files themselves is also verified.

By default, the integrity verification utility is located in the /opt/kaspersky/epagent/sbin directory.

To run the integrity verification utility:

1. Run the command line terminal on the device.
2. Run the command: `./integrity_checker --signature-type kds-with-filename [other parameters] [<path to the manifest>]`.

   As a result, the terminal will display verification statistics as well as a return code:

- `0` means the integrity of Kaspersky Endpoint Agent manifest and files is maintained
- `1` means this is not the case

Parameters and arguments are listed below.

`<path to the manifest>`

This argument is used to verify the integrity of the manifest located at the specified path. If this parameter is not specified, the utility uses the integrity_check.xml file in the utility directory as the manifest file.

`--verbose`

This parameter is used to display integrity verification results for each file and a verbose description of integrity errors, if any.

`--trace <path to the file>`

This parameter is used to specify a file for saving trace data at the DEBUG level.

If this parameter is not specified, trace data is not saved.

`--crl <path to the list of revoked certificates>`

This parameter is used to verify the signature of the manifest using a list of revoked certificates located at the specified path.

Creating a backup copy and restoring the program from backup

If you are using the non fault-tolerant version of Kaspersky Anti Targeted Attack Platform, you can create a backup copy of the program and then restore it from the backup copy.

For a standalone Central Node server, you can create a backup copy of the data from this Central Node server.

If you are using the distributed solution and multitenancy mode, you can:

- Create a backup copy of PCN data.
- 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. • The program database on Central Node: • Alerts and VIP statuses of alerts • Tasks and task execution results • Policies • User-defined TAA (IOA) rules and exclusions • User-defined IDS rules and exclusions • IOC files • Scan exclusion rules • Information about files in Storage • Information about quarantined objects • List of computers with Endpoint Agent • Reports and report templates • User account data • Notifications	Central Node settings, if selected. Program databases, by default.	Standalone Central Node server.
4 GB	PCN settings.	Custom	Distributed solution and multitenancy mode.
4 GB	SCN settings.	Custom As for a standalone Central Node server.	Distributed solution and multitenancy mode.

Maximum data volume	Data type	Exported data	Program operation mode
4 GB	Program databases on the PCN: • Alerts and VIP statuses of alerts • Task execution results • Policies • User-defined TAA (IOA) rules and exclusions • User-defined IDS rules and exclusions • IOC files • List of data excluded from the scan • Information about files in Storage • Information about quarantined objects • List of Kaspersky Endpoint Agent hosts • Reports and report templates • User account data • Notifications	Default	Distributed solution and multitenancy mode.
No	Configuration files.	Yes	All modes.
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.

The versions of the program being restored must match the version of the program installed on the server. If the versions of the programs do not match, an error message is displayed when the program restoration is initiated, and the restoration process is terminated.

Creating a backup copy of Central Node server settings from the program administrator menu

To create a backup copy of the Central Node (PCN or SCN in distributed solution and multitenancy mode), do the following 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 server settings is created.

Downloading a file containing a backup copy of server settings 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 Central Node server settings to the hard drive of your computer.

To download a file containing a backup copy of the Central Node server settings 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 server settings 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 server settings is saved to the hard drive of your computer in the current directory.

Uploading a file containing a backup copy of server settings from your computer to the Central Node server

To upload a file containing a backup copy of server settings from the hard drive of your computer to the Central Node server, run the following command in Technical Support Mode:

```
scp <name of the file containing a backup copy of server settings 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 server settings 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 server settings is uploaded to the Central Node server in the current directory.

Restoring server settings from a backup copy using the program administrator menu

To restore Central Node server settings from a backup copy, you must first create a backup copy of current server settings. In case of an error when restoring server settings you will be able to use a backup copy of server settings.

To restore server settings 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 server settings.

   If the necessary file is not listed, upload the file containing the backup copy of the settings 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 server settings>**.
8. Press **ENTER**.

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

Server settings are restored from the selected file.

If the hardware configuration of the Central Node server on which the backup copy was created differs from the hardware configuration of the server on which you are planning to restore the server settings, you need to reconfigure the application scaling settings after restoring.

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:

```
kata-backup-restore backup
```

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, where <path> is the absolute path or relative path to the directory in which the file with the backup copy of the program is created.
No	`-c`	Clear the directory before saving the program backup file.
No	`-d <number of stored files>`	Specify the maximum number of files from the backup copy of the program stored in the directory, where <number> is the number of files.
No	`-e`	Save files in Storage.
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, the list of data excluded from the scan, 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 KATA5.0.sql for the backup copy of the program version 5.0.

Example:

Command for creating a backup copy of the program:

```
kata-backup-restore backup -b <path> -c -d <number of stored files> -e -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, 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.

The versions of the program being restored must match the version of the program installed on the server. If the versions of the programs do not match, an error message is displayed when the program restoration is initiated, and the restoration process is terminated.

To restore Kaspersky Anti Targeted Attack Platform from a backup copy, run the following command in Technical Support Mode of the server:

```
kata-backup-restore restore
```

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, where <path> is the full path to the file containing a backup copy of the program.
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:

```
kata-backup-restore restore -r <path> -l <filepath>
```

Updating Kaspersky Anti Targeted Attack Platform

You can upgrade Kaspersky Anti Targeted Attack Platform from version 4.1 to version 5.0. During the upgrade, a non fault-tolerant version of the program is installed.

If you used one NTP server to configure the date and time of the Central Node server, we recommend to delete that NTP server or configure integration with an additional NTP server before updating Kaspersky Anti Targeted Attack Platform. Otherwise, an error may occur during the update.

An unavailable or non-operational server may be used as the additional NTP server.

Updating 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 5.0.

   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. Updating the Central Node component.

   You can upgrade the component to version 5.0 only from version 4.1. If you are using an older version, you must upgrade it to 4.1 in the following order: 3.7 → 3.7.1, 3.7.1 → 3.7.2, 3.7.2 → 4.0, 4.0 → 4.1.

   To update the Central Node component on the server with this component, you must first run the script kata-upgrade-preparation. The script is included in the program distribution kit.

   If you are not using the distributed solution and multitenancy mode and are using a standalone Central Node server, you can upgrade 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 upgrade is complete, the PCN server belongs to the same tenant it belonged to before the upgrade.

   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 tenant 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 tenants.

b. Configure the access of user accounts with the **Senior security officer** and **Security officer** roles to those tenants 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 a tenant 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 updating 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. Updating the Sensor component installed on a standalone server.

   The program does not have a standard upgrade procedure. You must install the component version 5.0.

4. Updating the Kaspersky Endpoint Agent component:

   - Kaspersky Endpoint Agent for Windows.
   - Kaspersky Endpoint Agent for Linux.

Special considerations for updating Kaspersky Anti Targeted Attack Platform from version 4.1 to version 5.0

1. After updating Kaspersky Anti Targeted Attack Platform to version 5.0, you must add license keys again.
2. Custom widget layouts in the **Dashboard** section are **not** saved after the program update.
3. The settings of network interfaces are **not** saved. If you want to use network interfaces to receive mirrored SPAN traffic, you need to configure traffic capturing after the update.

4. Sensor and Sandbox component data are **not** preserved.

5. Central Node 5.0 is **not** compatible with Sensor and Sandbox components of earlier versions.

Upgrading Central Node installed on a server

Before installing the application upgrade package, it is recommended to first create a backup of the current state of each Central Node server to be updated and download it to the hard drive from the application administrator menu. If installing an application upgrade package fails, or if you need to reinstall Kaspersky Anti Targeted Attack Platform, you can use the backup copy of the application.
We also recommend learning about the limitations of the version to which you are upgrading.

If you are using the distributed solution and multitenancy mode, you need to upgrade each Central Node in accordance with the following procedure without disconnecting the SCNs from the PCN.

The disconnection of SCNs from the PCN is irreversible, you cannot reconnect an SCN to any PCN server.

The upgrade is delivered as an upgrade package. The package is included in the application distribution kit.

To upgrade Central Node installed on a server:

1. Remove connectors, integration servers, external systems from the list of systems allowed for integration, as well as Sandbox and Sensor components installed separately from the Central Node being updated.

   All steps described below must be performed on servers in Technical Support Mode after elevating user privileges using the `sudo -i` command.

2. If you have upgraded Central Node to version 7.0.3 from version 6.1 or earlier, run the following commands:

   ```
   rm -rf /data/upgrade/
   rm -rf /opt/upgrade_venv
   ```

   If you never upgraded to version 7.0.3, skip this step.

3. Place the application upgrade package on the Central Node server in the `/data` directory.

4. Sign in to the management console of the Central Node server where you want to perform the upgrade via SSH or through the terminal.

5. Make sure you have more than 100 GB of free space on the /dev/sda2 partition.

6. Unpack the upgrade archive:

   - To upgrade to version 7.1.1:

     ```
     tar xvf /data/kata-upgrade-7.1.1.531-x86_64_en-ru-zh.tar.gz -C /data/
     ```

- To upgrade to version 7.1.2:

  ```
  tar xvf /data/kata-upgrade-7.1.2.532-x86_64_en-ru-zh.tar.gz -C /data/
  ```

7. Install the upgrade package by running the following commands:

   ```
   cd /data/upgrade/
   ./run_kata_upgrade.py
   ```

   The user name entry window is displayed.

8. In the displayed window, in the **Username** field, enter the name of the user with administrator rights, select the **OK** button and press **Enter**.

   Default value: **admin**.

9. In the displayed window, in the **Password** field, enter the password of the user with administrator rights, select the **OK** button and press **Enter**.

   This opens the window for entering the path to the update archive.

10. This opens a window; in that window, in the **Data directory** field, enter the path to the update archive, select the **OK** button and press **Enter**.

    Default value: **/data/upgrade**

11. In the displayed window, select the localization language for the NDR functionality.

    Parts of the application related to NDR functionality will be displayed in the selected language.

    After some time, the console will display a message prompting you to power off the server.

12. After the message prompting you to power off the server is displayed, run the following command:

    ```
    poweroff
    ```

13. Mount the Ubuntu-based ISO image of Kaspersky Anti Targeted Attack Platform 7.1.1 (kata-cn-7.1.1.531-inst.x86_64_en-ru-zh.iso). If you are using Kaspersky Anti Targeted Attack Platform based on the Astra Linux operating system, follow the instructions to create an ISO image.

14. Boot from the device that has the mounted iso image.

15. In the GRUB menu, select **Upgrade KATA 7.0.3**.

16. Follow the remaining steps of the wizard to complete the upgrade on the server.

17. When the upgrade finishes, sign in to the management console of the Central Node server where you performed the upgrade via SSH or through the terminal.

18. Delete the temporary files of the installer by running the following command:

    ```
    rm -rf /data/upgrade /data/install_data
    ```

19. Run the following command:

    ```
    docker exec -it $(docker ps | grep nta_database | awk '{print $1}') psql -p 5433 -U postgres -d kics -c 'GRANT SELECT ON TABLE kics_webserver.wl_rule_attributes TO kics_webserver;'
    ```

The Central Node component is upgraded.

After upgrading, you must log in again to the Central Node server management console over SSH or through

the terminal.

Special considerations involved in upgrading Central Node 7.0.3 on an Astra Linux server

When upgrading Central Node 7.0.3 on an Astra Linux server, more disk space may be required. If there is not enough disk space, the upgrade process is aborted and a message about insufficient disk space is displayed.

To resume the upgrade if there is not enough disk space:

1. Create a backup copy of Central Node and download it to your hard drive from the administrator menu of the application.
2. Clean up the disk using the utility.

After cleaning up the disk, you can resume the upgrade.

Restoring the Embedded Sensor after the upgrade in distributed solution and multitenancy mode

Embedded Sensor may be missing after upgrading a Central Node component that had been used in the distributed solution or multitenancy mode to version 7.1.1, 7.1.2 or 7.1.3.

To remove the limitation:

1. If, after upgrading the Central Node component, the Embedded Sensor is present but dsabled, remove Sensor in the web interface.
2. Sign in to the management console of the Central Node server on which you want to upgrade the Embedded Sensor over SSH or using a terminal.
3. When the system prompts you, enter the administrator user name and the password that was specified during installation of the component.

   The application component administrator menu is displayed.
4. In the application administrator menu, select Technical Support Mode.
5. Press ENTER.
6. This opens the Technical Support Mode confirmation window.
7. Confirm that you want to manage the application in Technical Support Mode. To do so, select Yes and press ENTER.
8. Run the following command:

   ```
   docker service update --cap-add=CAP_DAC_OVERRIDE --cap-add=CAP_IPC_LOCK --cap-add=CAP_SYS_PTRACE kata_product_main_1_preprocessor_span
   ```

9. If the Embedded Sensor was not restored, clear the databases by running the following command:

```
kata-sensor-tool reset-core
```

The Embedded Sensor is restored after approximately one minute.

Contents and amount of information kept when updating Kaspersky Anti Targeted Attack Platform

Information about the contents and amount of data kept when updating Kaspersky Anti Targeted Attack Platform from version 4.1 to version 5.0 is listed in the following table.

Contents and volume of data saved when updating the program from version 4.1 to version 5.0

Data type	Data saved during upgrade
Central Node or PCN settings.	All data except: • License keys • Settings for integration with the Sandbox component • Settings for integration with the Sensor component
Program database on Central Node or PCN (alert database, program operation monitoring data, custom rule database, tasks, policies, rules added to exclusions).	All data except: • Files in the scan queue when Kaspersky Anti Targeted Attack Platform is upgraded to version 5.0. • Files in the rescan queue when Kaspersky Anti Targeted Attack Platform is upgraded to version 5.0. • Report data.
Events database.	All data.
Storage and Quarantine	All data.
Sandbox artifacts.	All data.

Interaction with external systems via API

You can set up the integration of Kaspersky Anti Targeted Attack Platform with external systems to manage Threat Response actions, 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. For authorization, the program administrator must create a request to integrate the external system with the program. Then the administrator must process the request in the web interface of Kaspersky Anti Targeted Attack Platform.

If you have deployed the Central Node and Sensor components as a cluster, you can configure fault-tolerant integration with an external system using one of the following options:

- Using the Round Robin function.
- Configure the external system settings so that if a timeout occurs, the external system switches between the IP addresses of the cluster servers.

To configure the fault-tolerant integration with the external system:

1. Configure Round Robin on the DNS server for the domain name corresponding to the Central Node cluster.
2. Specify this domain name in the mail server settings.

   Integration with the mail server will be configured based on the domain name. The mail server will communicate with a random server in the cluster. If this server fails, the mail server will communicate with another healthy server in the cluster.

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 an external system with Kaspersky Anti Targeted Attack Platform:

1. Generate a unique identifier of the external system for authorization in Kaspersky Anti Targeted Attack Platform – `sensorId`.
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.

For scanning objects stored in external systems, the following Kaspersky Anti Targeted Attack Platform interaction scenario is recommended:

1. **Creating a request for scanning objects using the `HTTP POST` method**
2. **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.

3. **Creating a request to delete scan results using the HTTP method `DELETE`**

   You can delete the results of scanning a specified object or all objects.

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>:<port, 443 by
default>/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.

Settings

Parameter	Type	Description
`sensorId`	UUID	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. If this parameter is not defined, viewing scan results is not available.

Parameter	Type	Description
`objectType`	string	Type of scanned object. 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>:<port, 443 by
default>/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 application will display only the object scan requests that are being processed or in which the application has detected a threat.

Settings

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. Indicate one or more statuses separated by commas. The following parameter values are available: • `detect` • `not detected` • `processing` • `timeout` • `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.

Response

HTTP code: 200

Format: JSON

```
type Response []Scans

type Scans struct {
ScanID integer `json:"scanId"`
State array `json:"state"`
}
```

Returned value

Return code	Description
`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/state?sensorInstanceId=instance1&state=detect,not%20detected,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>:<port, 443 by
default>/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.

Settings

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 application'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>:<port, 443 by default>/kata/scanner/v1/sensors/<sensorId>/scans/filters"
```

If the request is processed successfully, the application'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.

Settings

Parameter	Type	Description
`sensorId`	string	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.

Response

HTTP code: 200

Format: JSON

```
type Response struct {
MaxObjectSize integer `json:"maxObjectSize"`
Version string `json:"version"`
}
```

Returned value

Return code	Description
`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 that external systems can use to receive information about application alerts

Kaspersky Anti Targeted Attack Platform provides an API that lets external systems access information about all alerts of the application 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 application 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 application runs in distributed solution mode, you must separately configure the integration with the external system for each PCN and SCN server from which you want to receive information about alerts. This limitation is due to the fact that the web interface of the PCN server displays information about all alerts, but the alerts database stores only those alerts that have been registered on that specific server.

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>:<port, 443 by default>/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.

Settings

Parameter	Type	Description
`sensorId`	String	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
`detect_type`	Array	The technology that created the alert. You can specify a comma-separated list of technologies. Possible values: • `am` – Anti-Malware Engine • `sb` – Sandbox • `yara` – YARA • `url_reputation` – URL Reputation • `ids` – Intrusion Detection System 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 10,000. 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. If this parameter is not specified, information about all alerts is provided.

Response

HTTP code: 200

Format: JSON

```
type Response struct {
Detects array `json:"detects"`
Token string `json:"token"`
}
```

Returned value

Return code	Description
`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 detection is listed in the following table.

Scope of information transmitted for an alert

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: • `high` • `medium` • `low`	Alert importance.
`objectSource`	One of the following values: • `web` • `mail` • `endpoint` • `external` • `dns`	Source of the detected object.
`technology`	One of the following values: • `am` – Anti-Malware Engine • `sb` – Sandbox • `yara` – YARA • `url_reputation` – URL Reputation • `ids` – Intrusion Detection System	Technology that was used to detect the object.
`objectType`	One of the following values: • `file`. • `URL`. • `host` (for remote domains or hosts).	Type of detected object.
`object`	Depends on the type of detected object.	Data on the detected object.
`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.	7bbfc1d690079b0c591e146c4294305da1cee857e12db40f431
	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. 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: • Anti-Malware Engine. • YARA. • Intrusion Detection System.	`detect`	List of detected threats.	Array	`HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic`
	`dataBaseVersion`	Version of databases used to scan the file.	Integer	`201811190706`
Sandbox	`detect`	List of detected threats.	Array	`HEUR:Trojan.Win32.Generic, Trojan-DDoS.Win32.Macri.avy, UDS:DangerousObject.Multi.Generic`
	`image`	Name of the virtual machine image where the file was scanned.	String	`Win7`
	`dataBaseVersion`	Database version in the following format: `<version of the application 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)`

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. IDS technology detections do not have this parameter. For URL technology detections, 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'

Source of the object	Parameter	Description	Data type	Example
	`messageId`	Email message ID.	String	`1745028736.156014.1542897410859.JavaMail.svc_jira_poo`
• `endpoint` • `external`	`hostName`	Name of the computer on which the detection was generated.	String	`computername.example.com`
	`IP`	IP address of the computer on which the detection was generated.	IP address	`198.51.100.0`
`dns`	`sourceIp`	IP address of the computer which initiated the DNS connection.	IP address	`192.0.2.0`
	`destinationIp`	IP address of the computer with which the DNS connection was established (typically, a DNS server).	IP address	`198.51.100.0`
	`destinationPort`	Port of the computer with which the DNS connection was established (typically, a DNS server).	Integer	`3128`
	`dnsMessageType`	Type of the DNS message: • `Request` • `Response`	String	`Request`
	`dnsRequestType`	One of the following DNS request types: • `A`. • `AAA`. • `CNAME`. • `MX`.	String	`MX`
	`domainToBeResolved`	Domain name from the DNS request.	String	`example.com`

API for managing Threat Response actions

Kaspersky Anti Targeted Attack Platform provides an API for performing Threat Response actions. Commands to carry out operations are received at the Central Node server and then relayed to the Endpoint Agent component.

You can use external systems to perform the following operations on hosts with the Endpoint Agent component:

- Manage network isolation of hosts
- Manage prevention rules
- Run applications

All of the above operations are available on hosts that use Kaspersky Endpoint Security for Windows in the role of the Endpoint Agent component.

If Kaspersky Endpoint Security for Linux is used in the role of the Endpoint Agent component, you can manage network isolation and run applications.

Request for getting the list of hosts with the Endpoint Agent component

To create a request for information about hosts with the Endpoint Agent component, the GET HTTP method is used.

Command syntax

GET "<URL of the Central Node server>:<port, 443 by default>/kata/response_api/v1/<external_system_id>/sensors"

If the request is processed successfully, a list of hosts with the Endpoint Agent component is displayed.

You can create a request for information about hosts with filters by IP address, name, or ID of the host. You can specify one, multiple, or all of these filters.

> When specifying a host name, you need to keep in mind that the filter is case-sensitive.

GET "<URL of the Central Node server>:<port, 443 by default>/kata/response_api/v1/<external_system_id>/sensors?ip=<IP address of the host>&host=<host name>&sensor_id=<sensor_id>"

If the request is processed successfully, information about the selected host with the Endpoint Agent component is displayed.

Settings

Parameter	Type	Description
external_system_id	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Unique ID of the host with the Endpoint Agent component
ip	string	IP address of the host with the Endpoint Agent component.
host	string	Name of the host with the Endpoint Agent component.

Example of entering commands with parameters

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors"
```

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/sensors?
ip=10.16.40.243&host=host4&sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0"
```

Response

HTTP code: 200

Format: JSON

```
type Response Sensors

type Server struct {
Version string `json:"version"`
},

type Sensors struct {
SensorID UUID `json:"sensorId"`
HostIP string `json:"hostIp"`
LastAccessTimestamp `json:"lastAccessTimestamp"`
Version string `json:"version"`
SelfDefenseState boolean `json:"selfDefenseState"`
LicenseStatus string `json:"licenseStatus"`
OSFamily string `json:"osFamily"`
OSName string `json:"osName"`
Capabilities array `json:"capabilities"`

}
```

Returned value

Return code	Description
400	Authorization required.
401	Incorrect parameters.
500, 502, 503, 504	Internal server error. Repeat the request later.

Request for information about network isolation and the existence of prevention rules for hosts with the Kaspersky Endpoint Agent component

HTTP method GET is used to create a request to display information about network isolation and the existence of prevention rules for hosts with the Endpoint Agent component.

Command syntax

```
GET "<URL of the Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=<network_isolation or prevention>"
```

If the request is processed successfully, the list of hosts with the Endpoint Agent component is displayed, listing hosts that had prevention rules or network isolation rules applied at the moment when the request was processed.

Settings

Parameter	Type	Description
`external_system_id`	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Unique ID of the host with the Endpoint Agent component
`settings_type`	enum	Rule type: network_isolation or prevention.

Example of entering a command with switches

```
GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

Response

HTTP code: 200

Format: JSON

```
type Response []Settings

type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec int `json:"autoTurnoffTimeoutInSec"`
}
```

Returned value

Return code	Description
400	Authorization required.
401	Incorrect parameters.
404	Specified hosts with the Endpoint Agent component not found.
500, 502, 503, 504	Internal error. Repeat the request later.

Host network isolation management

To isolate a host with the Endpoint Agent component using the API, the following procedure is recommended for interacting with Kaspersky Anti Targeted Attack Platform:

1. Creating a request for getting the list of hosts with the Endpoint Agent component
2. Creating a request for getting information about hosts that already have network isolation enabled
3. **Creating a request for one of the following operations with hosts with the Endpoint Agent component:**
   - Enable network isolation
   - Disable network isolation
   - Add an exclusion to an existing network isolation rule

You can manage the created network isolation rules in the web interface of the application.

Request to enable network isolation

To enable network isolation for a selected host, you must add a network isolation rule. To create the request, the HTTP POST method is used.

Command settings are passed in the body of the request in JSON format.

Command syntax

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST "
<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=network_isolation" -H 'Content-Type: application/json' -d '

{

"settings": {
```

```
"autoTurnoffTimeoutInSec": <network isolation time period>}

}

'
```

If the request is processed successfully, the network isolation rule is added. Network isolation for the selected host becomes active at the moment when the rule is added.

After a period of time specified when the request is created, network isolation becomes inactive. The network isolation rule itself is not deleted. If necessary, you can delete the selected rule.

To disable network isolation, you must create a request to disable the selected rule.

Settings

Parameter	Type	Description
`external_system_id`	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Unique ID of the host with the Endpoint Agent component
`autoTurnoffTimeoutInSec`	integer	Period of time during which the network isolation will be active. Allowed range - 1 to 9999 hours. Network isolation time period is specified in seconds. For example, if you want to enable network isolation of a host for two hours, you must specify 7200 seconds.

Example of entering a command with switches

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings": {
"autoTurnoffTimeoutInSec": 7200}
}
'
```

Response

HTTP code: 200

Format: JSON

```
type Response []Settings

type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec integer `json:"autoTurnoffTimeoutInSec"`
}
```

Returned value

Return code	Description
400	Incorrect parameters.
401	Authorization required.
404	Specified hosts with the Endpoint Agent component not found.
500, 502, 503, 504	Internal server error. Repeat the request later.

If you want to edit the settings of the created network isolation rule, you must create a new request to add the rule with the new settings.

Request to disable network isolation

To disable network isolation for a selected host, you must create a request to disable the network isolation rule. HTTP method DELETE is used to create the request.

Command syntax

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X DELETE
"<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=network_isolation"
```

If the request is processed successfully, the network isolation rule is disabled.

Settings

Parameter	Type	Description
external_system_id	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Unique ID of the host with the Endpoint Agent component

Example of entering a command with the DELETE parameter

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"
```

To verify that network isolation is disabled, make a request for information about a task using the HTTP GET method.

Example of entering a command with the GET parameter

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation"| python -m json.tool
```

If network isolation is disabled, Kaspersky Anti Targeted Attack Platform returns a response to the external system in the following format:

```
{
"error": "Not Found"
}
```

Returned value

Return code	Description
400	Incorrect parameters.
401	Authorization required.
404	Specified hosts with the Endpoint Agent component not found.
500, 502, 503, 504	Internal server error. Repeat the request later.

Request to add an exclusion to a network isolation rule

To add an exclusion to a previously created network isolation rule, you must create a request to add an exclusion. To create the request, the HTTP POST method is used.

Command settings are passed in the body of the request in JSON format.

Command syntax

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST "
<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=
<sensor_id>&settings_type=network_isolation" -H 'Content-Type: application/json' -d '

{
"settings":
{"excludedRules": [
{
"direction": "<outbound, inbound, or both>",
"protocol": <number of the IP protocol>,
"remoteIpv4Address": "<IP address of the host with the Endpoint Agent component whose
traffic must not be blocked>",
"localPortRange":
{
"fromPort": <port number>,
"toPort": <port number>
}
}
,
{
"direction": "<outbound, inbound, or both>",
"protocol": <number of the IP protocol>,
"remoteIpv4Address": "<IP address of the host with the Endpoint Agent component whose
traffic must not be blocked>",
"remotePortRange":
{
"fromPort": <port number>,
"toPort": <port number>
}
}
,
{
"direction": "<outbound, inbound, or both>",
"protocol": <number of the IP protocol>,
"remoteIpv4Address": "<IP address of the host with the Endpoint Agent component whose
traffic must not be blocked>"
}
]
,
"autoTurnoffTimeoutInSec": <network isolation duration>
}
}
'
```

If the request is processed successfully, the exclusion from the network isolation rule is added.

Settings

Parameter	Type	Description
`external_system_id`	`UUID`	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
`sensor_id`	`UUID`	Unique ID of the host with the Endpoint Agent component
`direction.`	`array`	Direction of network traffic that must not be blocked. Possible values: • inbound • outbound • both If you do not specify a value for this parameter, the default value is 'both', which means the application transmits traffic in both directions.
`protocol`	`integer`	IP protocol number assigned by the Internet Assigned Numbers Authority (IANA). If you do not specify a value for this parameter, by default, network isolation is applied to all protocols.
`remoteIpv4Address`	`string`	IP address of the host with the Endpoint Agent component whose traffic must not be blocked
`remotePortRange`	`string`	Destination port. You can specify a destination port only if you have selected an outbound direction of network traffic. Port ranges cannot be specified for bidirectional traffic.
`localPortRange`	`string`	Port from which the connection is initiated. You can specify a destination port only if you have selected an inbound direction of network traffic. Port ranges cannot be specified for bidirectional traffic.
`autoTurnoffTimeoutInSec`	`integer`	Period of time during which the network isolation will be active. Allowed range - 1 to 9,999 hours. Network isolation time period is specified in seconds. For example, if you want to enable network isolation of a host for two hours, you must specify 7,200 seconds.

Example of entering a command with switches

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?sensor_id=DF64838B-
B518-414B-B769-2B8BE341A2F0&settings_type=network_isolation" -H 'Content-Type: application/json' -d '
{
"settings":
{"excludedRules": [
{
"direction": "inbound",
"protocol": 6,
"remoteIpv4Address": "10.16.41.0",
"localPortRange":
{
"fromPort": 3389,
"toPort": 3389
}
}
,
{
"direction": "outbound",
"remoteIpv4Address": "10.16.41.1",
"remotePortRange":
{
"fromPort": 13957,
"toPort": 55409
}
}
,
{
"direction": "both",
"protocol": 6,
"remoteIpv4Address": "10.16.41.2"
}
]
,
"autoTurnoffTimeoutInSec": 7200
}
}
'
```

Response

HTTP code: 200

Format: JSON

```
type Response []Settings
type Settings struct {
ExcludedRules array `json:"excludedRules"`
AutoTurnoffTimeoutInSec integer `json:"autoTurnoffTimeoutInSec"`
}
type ExcludedRules struct {
Direction array `json:"direction"`
Protocol integer `json:"autoTurnoffTimeoutInSec"`
RemotePortRange string `json:"remotePortRange"`
LocalPortRange string `json:"localPortRange"`
}
```

Returned value

Return code	Description
`400`	Incorrect parameters.
`401`	Authorization required.
`404`	Specified hosts with the Endpoint Agent component not found.
`500, 502, 503, 504`	Internal server error. Repeat the request later.

If you want to edit the settings of the created exclusion, you must create a new request to add the exclusion with the new settings.

Managing prevention rules

You can use prevention rules to prevent files or processes from running on a selected hosts or all hosts with the Endpoint Agent component. For example, you can block certain applications that you consider insecure. The application identifies files based on their hash by using the MD5 and SHA256 hashing algorithms. A prevention rule created through external systems can contain multiple file hashes.

You can use external systems to manage all prevention rules created for a single host or all hosts at the same time. When you create a prevention rule for a selected host through external systems, Kaspersky Anti Targeted Attack Platform replaces all prevention rules applied to this host with a prevention rules with new parameters. For example, if you had added multiple prevention rules for a selected hosts through the application's web interface, and subsequently added a prevention rule through external systems, all prevention rules added in the web interface are replaced with the rule added through external systems.

When the parameters of a prevention rule created through external systems are modified, the application saves only the new parameters. For example, if you have added a prevention rule that contains hashes for multiple files, and want to add another hash to that rule, you must create a request to add a prevention rule and specify all hashes for which you had a prevention previously, plus the new hash.

The described scenario is also relevant for prevention rules applied to all hosts.

To create a prevention rule using the API, the following procedure is recommended for interacting with Kaspersky Anti Targeted Attack Platform:

1. Creating a request for getting the list of hosts with the Endpoint Agent component
2. Create a request for getting information about hosts that already have prevention rules.
3. **Create a request for one of the following operations with prevention rules:**
   - Create rule
   - Delete rule

Added prevention rules are displayed in the web interface of the application in the **Prevention** section, **Prevention rules** subsection.

If you are creating a prevention rule for all hosts through an external system, you must first make sure that no prevention rule for the same file exists on the server or is applied to one or multiple hosts. This prerequisite is also relevant if you want to create a prevention rule through an external system for a selected host: you must make sure that a prevention rule for the same file does not exist on the server and is not applied to all hosts. Otherwise, the server returns an error to the external system with a list of hosts that already have a prevention rule applied.

If the prevention rule created through an external system contains multiple file hashes, the error information mentions only the first file that caused the error. Information about other duplicated prevention rules is not displayed.

To modify a prevention rule previously created through the web interface or external systems, you must create a request to add a prevention rules with updated parameters.

Request to create a prevention rule

To create the request, the HTTP POST method is used. Command settings are passed in the body of the request in JSON format.

Command syntax

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST "
<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id or all,
if you want to create the prevention rule for all hosts>&settings_type=prevention" -H
'Content-Type: application/json' -d '

{

"settings": {

"objects": [

{

"file": {

"<sha256 or md5>": "<SHA256- or MD5-hash of the file that you want to prevent from
starting>"

}

},

{
```

```
"file": {

"<sha256 or md5>": "<SHA256- or MD5-hash of the file that you want to prevent from
starting>"

}

}

]

}

}

'
```

If the request is processed successfully, the prevention rule is added. The prevention rule becomes active at the moment when it is added.

If necessary, you can delete the prevention rule.

Settings

Parameter	Type	Description
`external_system_id`	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Unique ID of the host with the Endpoint Agent component
`objects`	string	Type of the object that you want to prevent from running. Possible value of the parameter: file.
`sha256 or md5`	string	SHA256 or MD5 has of the object that you want to prevent from running.

Example of entering a command with switches

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{
"settings": {
"objects": [
{
"file": {
"sha256": "830195824b742ee59390bc5b9302688c778fc95a64e7d597e28a74c03a04dd63"
}
},
{
"file": {
"md5": "d8e577bf078c45954f4531885478d5a9"
}
}
]
}
}
'
```

Response

HTTP code: 200

Format: JSON

```
type Response []Objects

type Objects struct {
type file struct {
SHA256 string `json:"sha256"`
},
type file struct {
MD5 string `json:"md5"`
}
}
```

Returned value

Return code	Description
400	Incorrect parameters.
401	Authorization required.
404	Specified hosts with the Endpoint Agent component not found.
500, 502, 503, 504	Internal server error. Repeat the request later.

Request to delete a prevention rule

You can delete a prevention rule using a new request with blank values or a request with the DELETE parameter. POST and DELETE HTTP methods are used to create requests.

Command syntax for a new request

Command settings are passed in the body of the request in JSON format.

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST "
<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id or all,
if you want to delete the prevention rule for all hosts>&settings_type=prevention" -H
'Content-Type: application/json' -d '

{

"settings": {

"objects": []

}

}

'
```

Command syntax with the DELETE parameter

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X DELETE
"<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/settings?sensor_id=<sensor_id or all,
if you want to delete the prevention rule for all hosts>&settings_type=prevention"
```

Settings

Parameter	Type	Description
external_system_id	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Unique ID of the host with the Endpoint Agent component

Example of command for a new request

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X POST
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention" -H 'Content-Type: application/json' -d '
{

"settings": {

"objects": []

}

}

'
```

Example of entering a command with the DELETE parameter

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X DELETE
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"
```

If the request is processed successfully, the prevention rule is deleted.

To verify that the prevention rule is deleted, make a request for information about the prevention rule using the HTTP GET method.

Example of entering a command with the GET parameter

```
curl -k --cert <path to TLS certificate file> --key <path to private key file> -X GET
"https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/settings?
sensor_id=all&settings_type=prevention"| python -m json.tool
```

If the prevention rule was deleted, Kaspersky Anti Targeted Attack Platform returns a response to the external system in the following format:

```
{
"error": "Not Found"
}
```

Returned value

Return code	Description
400	Incorrect parameters.
401	Authorization required.
404	Specified hosts with the Endpoint Agent component not found.
500, 502, 503, 504	Internal server error. Repeat the request later.

Managing the application run task

To manage the application run task using the API, the following procedure is recommended for interacting with Kaspersky Anti Targeted Attack Platform:

1. Creating a request for information about settings, creation time, and completion status of the task
2. **Creating a request for one of the following operations with the task:**
   - Creating the task
   - Deleting the task

Added tasks are displayed in the web interface of the application in the **Tasks** section.

Request to obtain information about a task

To create a request for getting information about a task, the HTTP GET method is used.

Command syntax

```
GET "<URL of the Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/tasks/<task_id>?settings=<true or
false>"
```

If the request is processed successfully, information is displayed about settings, creation time, and completion status of the task.

Settings

Settings	Type	Description
external_system_id	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
sensor_id	UUID	Unique ID of the host with the Endpoint Agent component
task_id	UUID	Unique ID of the task.
settings	boolean	Possible values: • true. If you enter this value, information is displayed about settings, creation time, and completion status of the task. • false. If you enter this value, information about creation time and completion status of the task is displayed.

Example of entering a command with switches

```
GET https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=<true or false>
```

Response

HTTP code: 200

Format: JSON

```
type Response struct {
State `json:"state"`
LatestStartDateTime `json:"latestStartDateTime"`
type Task struct {
type Schedule struct {
StartNow boolean `json:"startNow"`
ExecCommand string `json:"execCommand"`
}
}
}
```

Returned value

Return code	Description
400	Incorrect parameters.
401	Authorization required.
409	The task with the specified ID was already exists.
500, 502, 503, 504	Internal server error. Repeat the request later.

Request to create a task

The HTTP POST method is used for requests to run the Kaspersky Anti Targeted Attack Platform application. Command settings are passed in the body of the request in JSON format.

Command syntax

```
curl -k --<path to the TLS certificate file> --key <path to private key file> -X POST "
<URL of Central Node server>:<port, 443 by
default>/kata/response_api/v1/<external_system_id>/tasks/<task_id>?sensor_id=
<sensor_id>&task_type=run_process" -H 'Content-Type: application/json' -d '

{

"task": {

"shedule": {"startNow": <true or false>},

"execCommand": "<name of the application that you want to run>",

"cmdLineParameters": "<additional options for running the file or command>",

"workingDirectory": "<working directory>"

}

}

'
```

If the request is processed successfully, the run application task is created.

Settings

Parameter	Type	Description
`external_system_id`	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
`sensor_id`	UUID	Unique ID of the host with the Endpoint Agent component
`task_id`	UUID	Unique ID of the task.

Example of entering a command with switches

```
curl -k --example.cert --example.key -X POST "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?sensor_id=DF64838B-B518-414B-B769-2B8BE341A2F0&task_type=run_process" -H 'Content-Type: application/json' -d '
{

"task": {

"schedule": {"startNow": true},

"execCommand": "Example.exe",

"cmdLineParameters": "C:\Windows\System32\",

"workingDirectory": "/all"

}

}

'
```

Response

HTTP code: 200

Format: JSON

```
type Response struct {
State `json:"state"`
LatestStartDateTime `json:"latestStartDateTime"`
type Task struct {
type Schedule struct {
StartNow boolean `json:"startNow"`
ExecCommand string `json:"execCommand"`
}
}
}
```

Returned value

Return code	Description
400	Incorrect parameters.
401	Authorization required.

Return code	Description
404	The task with the specified ID was not found.
500, 502, 503, 504	Internal server error. Repeat the request later.

If you want to edit the settings of the created task, you must create a new request to add the task with the new settings.

Request to delete a task

To create a request to delete a Kaspersky Anti Targeted Attack Platform task, the HTTP DELETE method is used.

Command syntax

```
curl -k --<path to TLS certificate file> --key <path to private key file> -X DELETE "<URL of the Central Node server>:<port, 443 by default>/kata/response_api/v1/<external_system_id>/tasks/<task_id>"
```

If the request is processed successfully, the application run task is deleted.

Settings

Parameter	Type	Description
external_system_id	UUID	Unique ID of the external system used for authorization in Kaspersky Anti Targeted Attack Platform.
task_id	UUID	Unique ID of the task.

Example of entering a command with the DELETE parameter

```
curl -k --example.cert --example.key -X DELETE "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8"
```

If the request is processed successfully, the prevention rule is deleted.

To verify that the task is deleted, make a request for information about the task using the HTTP GET method.

Example of entering a command with the GET parameter

```
curl -k --example.cert --example.key -X GET "https://10.10.0.22:443/kata/response_api/v1/15301050-0490-4A41-81EA-B0391CF21EF3/tasks/2EEB4CBC-10C6-4DC4-BE0A-72A75CDB0BE8?settings=false"| python -m json.tool
```

If the task was deleted, Kaspersky Anti Targeted Attack Platform returns a response to the external system in the following format:

```
{
"error": "Not Found"
}
```

Returned value

Return code	Description
`400`	Incorrect parameters.
`401`	Authorization required.
`404`	The task with the specified ID was not found.
`500, 502, 503, 504`	Internal server error. Repeat the request later.

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 about purchasing, installing, and using the application.

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.

Discussing Kaspersky software on the Forum

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on our Forum.

On the Forum, 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.

Obtaining information about Kaspersky Endpoint Agent for Linux for Technical Support

After you report a problem to Kaspersky Technical Support, they may ask you to generate a report with information about the operating system and send it to Kaspersky Technical Support. Kaspersky Technical Support may also ask you to create a trace file. The trace file allows you to trace the process of performing program commands step by step and determine the stage of program operation at which an error occurs.

Kaspersky Endpoint Agent enables system event audit using Linux Audit Daemon and sets up audit rules for itself. When the program is removed, audit rules configured by it are also removed. This does not stop Linux Audit Daemon.

To provide support more effectively in case of questions about the operation of the program, Technical Support staff can ask you to temporarily modify program settings during diagnostics to make debugging easier. To do so, you may have to:

- Retrieve extended diagnostic information.
- Fine-tune program settings in ways that are not possible with the standard user interface.
- Modify the settings for storing and sending the retrieved diagnostic information.
- Configure network traffic to be intercepted and saved to a file.

Technical Support staff 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, and other resources) and inform you about the scope of data obtained for debugging purposes. The retrieved diagnostic information 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 Help 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.

How to obtain Technical Support

If you cannot find a solution to your problem in the 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 you contact Technical Support, please read the technical support rules.

You can contact Technical Support in one of the following ways:

- Visit the Technical Support website.
- Send 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 software. 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.

Alert

A record of the detection or a set of detections made as a result of scanning the object with Kaspersky Anti Targeted Attack Platform modules and technologies. Displayed in the table of alerts.

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

Application core. 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

Application component. Scans data, analyzes the behavior of objects, and publishes analysis results in the web interface of the application.

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.

Detection

The result of an object being scanned by an individual module or component of the application.

Distributed solution

Two-level hierarchy of servers with Central Node components installed. This hierarchy allocates a primary control server *(Primary Central Node (PCN))* and secondary 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 application.

Endpoint Agent component

Application component. Installed on workstations and servers of the corporate IT infrastructure that run Microsoft Windows, Linux and macOS operating systems. Continuously monitors processes running on those computers, active network connections, and files that are modified.

ICAP client

The system through which Kaspersky Anti Targeted Attack Platform receives traffic.

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

Application 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 application considers the event to be a detection and creates 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 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 Kaspersky Anti Targeted Attack Platform which detects threats on the perimeter of the enterprise IT infrastructure.

KEDR

Kaspersky Endpoint Detection and Response. Functional block of Kaspersky Anti Targeted Attack Platform which provides protection for the local area network of the organization.

Kerberos authentication

A mechanism for mutual authentication of client and server before a connection is established between them, which allows communication over unprotected networks. The mechanism is based on using a ticket, which is issued to the user by a trusted authentication center.

Keytab file

A file containing pairs of unique names (principals) of clients that are allowed to use Kerberos authentication and encrypted keys derived from the user password. Systems that support Kerberos use keytab files to authenticate users without entering a password.

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.

MIB (Management Information Base)

Virtual database used to manage objects that are transmitted over the SNMP protocol.

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.

Kaspersky Anti Targeted Attack Platform supports receiving mirrored traffic from aggregating devices: a network packet broker or a network tap. If filtering is to be applied to traffic coming from aggregating devices, the hardware requirements of Kaspersky Anti Targeted Attack Platform must be adjusted. To determine the actual hardware requirements of the solution, we recommend doing a pilot deployment first.

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 Kaspersky Anti Targeted Attack Platform is used to protect the infrastructure of multiple organizations or branch offices of the same organization 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

Application 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

Application component. Receives data.

Service principal name (SPN)

Unique ID of the service on the network for Kerberos authentication.

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 a detection and creates 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

Application 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.

Tenant

An individual organization or branch office of an organization to which the Kaspersky Anti Targeted Attack Platform solution is being provided.

TLS encryption

Encryption of connection between two servers, which ensures secure transmission of data between servers on the Internet.

Tracing

The application is run in debugging mode; after each command is executed, the application is stopped and the result of this step is displayed.

VIP status

Status of detections with special access permissions. For example, alerts with the VIP status cannot be viewed by users with the **Security officer** role.

YARA

Application 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 application installation directory.

Trademark notices

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

Apple, Mac, Macintosh, and Safari are trademarks of Apple Inc.

Ubuntu® is a registered trademark of Canonical Ltd.

Snort is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Citrix™ is a trademark of Citrix Systems, Inc. and/or of its subsidiaries, and registered in the United States Patent and Trademark Office and in other countries.

ESET™ and ESET NOD32™ are trademarks or registered trademarks of ESET s.r.o. or another relevant ESET company.

Google and Google Chrome are trademarks of Google LLC.

Intel, Xeon and Core are trademarks of Intel Corporation in the U.S. and/or other countries.

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

McAfee is a trademark or registered trademark of McAfee LLC or its subsidiaries in the United States and other countries.

Microsoft, Active Directory, Excel, Internet Explorer, Microsoft Edge, PowerPoint, PowerShell, Win32, Windows, Windows Server, Windows Vista, and Windows XP are trademarks of the Microsoft group of companies.

Mozilla™ and Firefox™ are trademarks of the Mozilla Foundation in the United States and other countries.

Oracle is a registered trademark of Oracle and/or its affiliates.

Red Hat, CentOS and Red Hat Enterprise Linux are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

Symantec is a trademark or registered trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

Trend Micro is a trademark or registered trademark of Trend Micro Incorporated.

VMware ESXi™ is a trademark of VMware, Inc. or a registered trademark in the United States or other jurisdictions of VMware, Inc.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.