kaspersky

Kaspersky Endpoint Security for Linux 12.5.0

© 2026 AO Kaspersky Lab

Contents

Kaspersky Endpoint Security for Linux
About the application
Key features
What's new in version 12.5
Fixed issues
Hardware and software requirements
Distribution kit
Compatibility with other applications
Comparison of functionality across Kaspersky solutions
Deployment and initial configuration
Modes and deployment schemes
Preparing the environment for installing the application
Selecting the system event interception mechanism
Preparing distribution packages
Preparatory actions in Kaspersky Security Center
Installing the application using Kaspersky Security Center
Installing the application using the command line
Additional configuration steps after installation in certain operating systems
Migration scenario to Kaspersky Security Center for Linux using the fast installation script
Updating the application from a previous version
Updating Kaspersky Endpoint Security management plug-ins
Application settings after upgrade
Uninstalling the application
Using the application
Licensing
How to switch to another Kaspersky solution
Managing license keys
Viewing information about license keys
Management interfaces of the application
Managing the application using Kaspersky Security Center
Kaspersky Security Center policies
Policy management
Exporting and importing policy settings
Tasks for Kaspersky Endpoint Security created in Kaspersky Security Center
Logging in and out of the Web Console and Cloud Console
Managing the application using the command line
Kaspersky Endpoint Security local tasks
Editing task settings
Configuring the task schedule
Managing general application settings
Using filters to limit results of queries
Exporting and importing application settings
Managing the application via the graphical interface

Protection status monitoring
Real-Time Protection statuses
Events and reports
Configuring event logging to the operating system log
Configuring application event log settings
Viewing application events
Viewing reports
Obtaining system performance metrics
Application stability monitoring
Application components integrity check
Application access control
Predefined roles
How to assign or revoke a user role
RBAC functional areas in Kaspersky Security Center
Recommendations for typical roles of protected devices
Updating application databases and modules
How to select the update source and distribution scheme
How to configure the database update task
How to update using the Kaspersky Update Utility
How to roll back updates of application databases and modules
Host Threat Protection
File Threat Protection
How to create a protection scope
How to select an action on file threat detection
What is the Smart mode of file scanning
How to optimize file scanning
Special considerations for scanning symbolic links and hard links
Malware Scan
How to create a scan scope
How to configure a scan schedule
How to scan an individual file or directory
How to optimize custom scan tasks
Critical Areas Scan
Container Scan
How to configure integration with container management tools
How to create an on-demand scan scope for containers and images
How to optimize Container Scan
How to select an action to be performed on a container when an infected object is detected
How to run a custom scan of containers and images
Removable drives scan
Behavior Detection
Exploit Prevention
Anti-Cryptor
How to select an action on malicious encryption detection
How to create a protection scope

BadUSB Attack Prevention
How to configure USB device authorization
How to allow connecting USB devices using the on-screen keyboard
How to allow connecting USB devices using the barcode scanner
Communication & Web Protection
Mail Threat Protection
What to do if a mail threat is detected
How to optimize email attachment scanning
What an email attachment filter is for
Web Threat Protection
How to select an action on web threat detection
What is Anti-Phishing
Network Threat Protection
How to select an action on network threat detection
How to manage blocked devices
Firewall Management
How to create a network packet rule
Network packet rule usage examples
How to add an IP address to a network zone: Public, Local, Trusted
What are dynamic rules
How to create rules for connecting to Kaspersky Security Center
Security Controls
Device Control
How to manage the list of trusted devices on the command line
How to configure device access mode
How to configure device access rules
How to configuring the Device Control message template
Granting temporary access to device
Web Control
How to create a rule of access to web resources
How to modify Web Control message templates
Rules for creating web resource address masks
Application Control
Application inventory
How to configure the Application Control operating mode
Creating application categories
Golden Image
About Application Control rules
Application Control rules test mode
System Integrity Monitoring
Real-time System Integrity Monitoring
System Integrity Check
Trusted zone
How to add protection exclusions
How to add trusted web addresses
How to add a trusted IP address of a computer
How to select monitored network ports

How to add a certificate to the list of trusted root certificates
How to add a trusted domain
How to exclude mount points
How to add trusted applications
How to add trusted devices
General settings
Detection settings
Kaspersky Security Network
How to enable or disable Kaspersky Security Network
What is the cloud mode of the application
What is the purpose of the KSN Proxy
Configuring the transfer of data to Kaspersky Security Center storage
How to configure application startup
Configuring permissions for task management
Password protection
About custom permissions
Default user permissions
Performance settings
Network settings
How to manage proxy settings
How the application intercepts traffic
How to configure certificate validation policy
How to configure monitored ports
Exclusions from traffic interception using the tools of the operating system
Interception of file operations
Configuring system event interception
Managing additional telemetry settings
Backup
Protection against advanced threats and targeted attacks
Response actions
Searching for indicators of compromise
Network isolation
Manually enabling or disabling the network isolation of the device in the Web Console
Configuring the duration of automatic network isolation
Manually configuring network isolation
Configuring exclusions from network isolation in the Web Console
Quarantine file
Receiving a file from a device
Delete file from device
Start process
Terminate process
Execution prevention for objects
Managing the Quarantine
Endpoint Detection and Response Optimum
How to enable the EDR Optimum integration
How to verify that the EDR Optimum integration is up and running
Cloud Sandbox

Endpoint Detection and Response Expert (on-premises)
How to prepare a reference image for correct integration with EDR Expert (on-premises)
How to configure the EDR Expert (on-premises) integration
How to verify that the EDR Expert (on-premises) Integration is up and running
Endpoint Detection and Response Expert (cloud)
How to configure the built-in agent integration with EDR Expert (cloud)
How to optimize EDR Expert (cloud) telemetry transmission
How to configure EDR Expert (cloud) telemetry exclusions
How to export or import EDR Expert (cloud) event filters
Kaspersky Anti Targeted Attack Platform
How to configure the EDR (KATA) integration
How to configure the NDR (KATA) integration
How to verify that the KATA Integration is up and running
Sandbox
How to configure the Sandbox integration
How to verify that the Sandbox Integration is up and running
How to send a file to Sandbox manually
Kaspersky Managed Detection and Response
Recommendations for creating a reference image for correct integration with MDR
Uploading the KPSN configuration file
How to configure the MDR integration
How to verify that the MDR Integration is enabled
Kaspersky Unified Monitoring and Analysis Platform
How to configure the KUMA integration
How to verify that the KUMA Integration is up and running
Protection of virtual environments
How to configure SVM discovery
How Light Agent selects SVMs
How to balance the connection of Light Agents among SVMs
Protecting the connection between Light Agent and an SVM
How to find out the status of the Light Agent
Best practices
Optimizing resource consumption by the application
Analysis of application performance on the device
Recommendations for File Threat Protection and scan tasks
Recommendations for the Web Threat Protection and Network Threat Protection tasks
Recommendations for Behavior Detection
Interoperability with Kaspersky solutions
Kaspersky Security Center Linux
Network Detection and Response (KATA)
Kaspersky Unified Monitoring and Analysis Platform
Application components reference
Commands for managing Kaspersky Endpoint Security
Commands for managing license keys
Commands for managing users and roles

- Managing application tasks and settings
  - Commands for managing general application settings
  - Commands for managing task settings
  - Commands for managing tasks
  - Commands for managing general Container Scan settings
  - Commands for managing network traffic scan settings
- Status and protection monitoring
  - Statistics commands
  - Command for displaying events
  - Commands for managing application events
  - Command for managing system performance metrics
- Security Controls
  - Commands for managing Device Control
  - Commands for managing Application Control
  - Web Control management commands
- Network connection protection
  - Commands used to manage blocked devices
  - Commands for Firewall Management
- Protection against advanced threats and targeted attacks
  - Commands for managing the Quarantine
  - Commands for managing the EDR Expert (on-premises) component
  - Commands for managing the EDR Expert (cloud) component
  - Commands for managing the NDR (KATA) component
  - Commands for managing device network isolation
  - Commands for managing the KUMA integration settings
  - Commands for managing the Sandbox integration settings
  - Commands for managing IOC scans
- Application commands in Light Agent mode

Application command-line options
- Update task
- Host Threat Protection
  - File Threat Protection task
  - Optimizing network directory scanning
  - Malware Scan
    - Malware Scan task
    - Custom Scan task
  - Critical Areas Scan task
  - Removable drives scan task
  - Container Scan
    - Container Scan settings
    - Container scan task
    - Integration with Jenkins
  - Anti-Cryptor task
  - Behavior Detection task
  - Exploit Prevention

Using Kaspersky Security Network
Connecting to Kaspersky Security Network
Enabling or disabling cloud mode
BadUSB Attack Prevention task
Communication & Web Protection
Web Threat Protection task
Scanning network traffic
Viewing and editing network traffic scan settings
Viewing exclusions from encrypted connections scan
Managing the list of trusted root certificates
Configuring and viewing traffic interception exclusions
Network Threat Protection task
Firewall Management
Configuring the list of network packet rules
Configuring network zones
Security Controls
Device Control task
Web Control
Web Control task
Viewing and editing Web Control settings
Application Control
Application Control task
Creating and editing a list of categories
Viewing the list of categories
Configuring the Application Control rule list
Configuring Inventory
Inventory task
Viewing a list of detected applications
System Integrity Monitoring task
System Integrity Check task
Protection against advanced threats and targeted attacks
Kaspersky Endpoint Detection and Response Expert (on-premises) Integration
Kaspersky Endpoint Detection and Response Expert (on-premises) Integration settings
Managing certificates for connecting to OSMP EDR Expert (on-premises) servers
Kaspersky Endpoint Detection and Response Expert (cloud) integration
Kaspersky Endpoint Detection and Response Expert (cloud) integration settings
Managing OSMP EDR Expert servers (cloud) connection certificates
Kaspersky Endpoint Detection and Response (KATA) Integration
Kaspersky Endpoint Detection and Response (KATA) integration settings
Managing certificates for connecting to the KATA server
Kaspersky Network Detection and Response (KATA) Integration
Kaspersky Network Detection and Response (KATA) integration settings
Managing certificates for connecting to the NDR server
Sandbox Integration
Sandbox integration settings
Managing certificates for connecting to the Sandbox server
Enabling or disabling Kaspersky Endpoint Detection and Response Optimum integration

Configuring the Kaspersky Managed Detection and Response integration
Managing device network isolation
Managing Quarantine settings
Managing quarantined files on the command line
Searching for indicators of compromise
Managing Execution prevention
Configuring KUMA integration
Kaspersky Unified Monitoring and Analysis Platform Integration task
Managing certificates for connecting to the KUMA server
General settings
General application settings
Task schedule
Configuring proxy server settings
Configuring Backup settings
Network traffic scan settings
Configuring global exclusions
Password protection settings
Application settings in the Administration Console
Database update
Host Threat Protection
File Threat Protection
Scan scopes window
New scan scope window
Scan settings window
Actions on threat detection window
File Threat Protection exclusions
Exclusion scopes window
New exclusion scope window
Exclusions by mask window
Exclusions by threat name window
Exclusions by process window
Trusted process window
Malware Scan
Scan scopes window
<New scan scope> window
Scan scope settings window
Scan scopes window
Scan settings window
Actions on threat detection window
Exclusions section
Exclusion scopes window
New exclusion scope window
Exclusions by mask window
Exclusions by threat name window
Critical Areas Scan
Scan scopes window
New scan scope window

- Scan scope settings window
- Scan scopes window
- Scan settings window
- Actions on threat detection window
- Exclusions section
- Exclusion scopes window
- New exclusion scope window
- Exclusions by mask window
- Exclusions by threat name window
- Container monitoring
  - Container Scan settings window
- Container Scan
  - Container Scan settings window
  - Scan settings window
  - Actions on threat detection window
  - Exclusions section
  - Exclusions by mask window
  - Exclusions by threat name window
- Removable drives scan
- Behavior Detection
  - Exclusions by process window
  - Trusted process window
- Exploit Prevention
  - Exploit Prevention exclusions window
  - Exploit Prevention exclusion window
- Anti-Cryptor
  - Scan scopes window
  - New scan scope window
  - Protection settings window
  - Exclusion scopes window
  - New exclusion scope window
  - Exclusions by mask window
- Kaspersky Security Network
  - Kaspersky Security Network settings
  - Kaspersky Security Network Statement
  - Kaspersky Private Security Network Statement
- BadUSB Attack Prevention
- Communication & Web Protection
- Mail Threat Protection
  - Mail Threat Protection settings window
  - Attachment filter window
- Web Threat Protection
  - Trusted web addresses window
  - Scan settings window
- Network Threat Protection
  - Exclusions window

- Firewall Management
  - Network packet rules window
  - Added network packet rule window
  - Add IP addresses window
  - Available networks window
  - Network connection window
- Security Controls
  - Device Control
    - Trusted devices window
    - Trusted device (Device ID) window
    - Device window on client devices
    - List of devices based on Device Control events window
    - Access to trusted device window
    - User or group window
    - Device type window
    - Configure device access rule window
    - User or group window
    - Access schedule window
    - Connection buses window
  - Web Control
    - Web Control rule window
    - Content category selection window
    - Data type category selection window
    - Select addresses window
    - Select address groups window
    - Add address group window
    - Select users window
    - User or group window
    - Access schedule window
  - Application Control
    - Application Control rules window
    - Adding rule window
    - Application categories window
    - User or group window
    - Inventory
      - Scan scopes window
      - New scan scope window
      - Exclusions section
      - Exclusion scopes window
      - New exclusion scope window
  - System Integrity Monitoring
    - Scan scopes window
    - New scan scope window
    - Exclusion scopes window
    - New exclusion scope window
    - Exclusions by mask window

System Integrity Check
Scan scopes window
New scan scope window
Exclusions section
Exclusion scopes window
New exclusion scope window
Exclusions by mask window
Local Tasks
Task management
Protection against advanced threats and targeted attacks
Integration with Kaspersky Managed Detection and Response
Kaspersky Endpoint Detection and Response (on-premises) Integration
Configuring the KATA server connection
Managing general KATA server connection settings
Configuring data transmission to KATA servers
Kaspersky Network Detection and Response (KATA) Integration
Configuring the NDR server connection
Managing general NDR server connection settings
Configuring data transmission to NDR servers
Integration with KUMA
KUMA servers window
KUMA server window
KUMA server connection settings window
Adding a server certificate window
Adding a client certificate window
Quarantine
Execution prevention for objects
General settings
Proxy server
Proxy server exclusions window
CPU usage by scan tasks
Running tasks on battery power
Starting the application
Automatically restarting when a critical update is received
Password protection
Trace and dump settings
Resident memory usage by the application
Encrypted connections scan
Trusted domains window
Trusted certificates window
Traffic interception exclusions window
Traffic interception exclusion window
Monitored ports
Global exclusions
Mount point path window
Excluding process memory from scans
Backup

Detection of applications that hackers can use to harm
Interception of file operations
Sending information to Kaspersky Security Center storage
System event interception
Additional telemetry settings
Light Agent mode
Connection to the Integration Server
Connection to the Integration Server window
Verify Integration Server certificate window
Authentication on the Integration Server window
SVM discovery settings
SVM connection tag
SVM selection algorithm
Protecting the connection
Known issues and limitations
Contact Technical Support
Technical Support via Kaspersky CompanyAccount
Obtaining information for Technical Support
How to enable and configure trace file creation
How to enable and configure dumping
Remote device diagnostics using Kaspersky Security Center
Appendices
Appendix 1. Configuration files and default application settings
Rules for editing task configuration files
Initial configuration files
Initial configuration settings in the installation package
Preset configuration files
Default settings for command line tasks
Default settings for the File_Threat_Protection task (ID:1)
Default settings for the Scan_My_Computer task (ID:2)
Default settings for the Scan_File task (ID:3)
Default settings for the Critical_Areas_Scan task (ID:4)
Default settings for the Update task (ID:6)
Default settings for the System_Integrity_Monitoring task (ID:11)
Default settings for the Firewall_Management task (ID:12)
Default settings for the Anti_Cryptor task (ID:13)
Default settings for the Web_Threat_Protection task (ID:14)
Default settings for the Device_Control task (ID:15)
Default settings for the Removable_Drives_Scan task (ID:16)
Default settings for the Network_Threat_Protection task (ID:17)
Default settings for Container_Scan (ID:18) and Custom_Container_Scan (ID:19) tasks
Default settings for the Behavior_Detection task (ID:20)
Default settings for the Application_Control task (ID:21)
Default settings for the Inventory_Scan task (ID:22)
Default settings for KATAEDR task (ID:24)
Default settings for the Web_Control task (ID:26)
Default settings for the Standalone_Sandbox task (ID:29)

Default settings for KATANDR task (ID:31)
Default settings for the KUMA task (ID:33)
Default settings of the Mail Threat Protection task (ID: 35)
Default settings of the BadUSB Attack Prevention task (ID: 37)
Default settings for KATANDR task (ID:31)
Appendix 2. Configuring interaction with Kaspersky Anti-Virus for Linux Mail Server
Appendix 3. Settings for interaction with external services
Appendix 4. File extensions for quick removable drives scan
Appendix 5. Variables in message templates
Appendix 6. Application events
Critical
Warning
Informational message
Appendix 7. Return codes
Appendix 8. Preparing an archive with application databases
Appendix 9. Requirements for IOC files
Legal notice
Data provision
Data provided when using an activation code
Data provided when downloading updates from Kaspersky update servers
Data transferred when using the application in Light Agent mode
Data sent to Kaspersky Security Center
Data provided when following links in the application interface
Data provided when using Kaspersky Security Network
Data provided when integrating with Kaspersky Endpoint Detection and Response Optimum
Data provided when integrating with the Kaspersky Endpoint Detection and Response (KATA) component
Data provided when integrating with the Kaspersky Endpoint Detection and Response Expert (on-premises) component
Data provided when integrating with the Kaspersky Endpoint Detection and Response Expert (cloud) component
Data provided when integrating with the Kaspersky Network Detection and Response (KATA) component
Data provided when integrating with Kaspersky Unified Monitoring and Analysis Platform
Information about third-party code
Trademark notices

Kaspersky Endpoint Security for Linux

Browse

Kaspersky Endpoint Security for Linux
What's new in version 12.5
Typical deployment schemes
Comparison of functionality
Known issues and limitations

Quick start

Hardware and software requirements
Compatibility
Preparing distribution packages
Preparing the environment for installation
Deploying the application
Migration scenario to Kaspersky Security Center Linux

Using the application

Activation
Updating databases
Updating using Kaspersky Update Utility
File Threat Protection
Trusted zone
Optimizing resources

Configuring in the command line

Managing the application using the command line
Management commands
Application command-line options

Support

Protection status monitoring
Upgrading a previous version of the application
Contacting Technical Support

About the application

Kaspersky Endpoint Security for Linux provides advanced comprehensive protection of Linux devices and allows preventing, detecting, and responding to various types of threats, network attacks, and fraud. The application is included in many Kaspersky multiplatform solutions and can be flexibly configured to match the challenges of your organization's IT infrastructure.

You can manage Kaspersky Endpoint Security installed on protected devices locally as well as centrally using Kaspersky Security Center.

The application is not intended for industrial processes that use automated control systems. To protect devices in these systems, we recommend using Kaspersky Industrial CyberSecurity for Linux Nodes.

Key features

Protection from mass cyber threats

Protection based on advanced technologies is the foundation of your IT security. Kaspersky Endpoint Security prevents file systems of user devices from becoming infected, monitors the connection of removable drives to the device and scans them for viruses. It monitors malicious activity of applications and protects files from malicious remote encryption. Databases with information about new global threats, for example, viruses, Trojans, cryptors, hacker attacks, are updated regularly and automatically.

Communication & Web Protection

Kaspersky Endpoint Security reliably protects the network environment of your organization: it scans email, websites and downloaded files for viruses, network worms and other threats before you open them. The application allows scanning incoming network traffic for activity that may indicate a network attack, monitors the settings of the operating system firewall and filters network activity.

Workplace security controls

By using Kaspersky Endpoint Security to control user access to applications, web resources, and connected devices at the workplace, you provide another layer of security for your organization. This helps protect devices from infection and prevent data loss or leaks.

Protection against advanced threats and targeted attacks

The application can interact with Kaspersky Detection and Response solutions, namely Kaspersky Managed Detection and Response (MDR) and Kaspersky Anti Targeted Attack Platform (KATA). The Kaspersky SIEM solution, Kaspersky Unified Monitoring and Analysis Platform (KUMA), is also supported. Kaspersky Endpoint Security monitors processes running on user devices, open network connections, and files being modified. Interaction with Detection and Response solutions provides protection against threats such as exploits, ransomware, fileless attacks, and legitimate system tools that hackers can use to compromise devices or data.

Protection of virtual and cloud environments

Kaspersky Endpoint Security as part of the Kaspersky Security for Virtualization Light Agent solution provides protection for virtual machines running Linux guest operating systems on a variety of server virtualization platforms and VDI platforms. Object scanning for viruses is performed by a special component installed on a separate virtual machine, the SVM (Secure Virtual Machine). Thus, the application provides security using the resources of the SVM instead of the resources of the virtual machine, which, together with smart optimization (for example, the use of a shared cache), minimizes the overall load on the IT infrastructure.

What's new in version 12.5

Kaspersky Endpoint Security 12.5 for Linux introduces the following features and improvements:

- Support for installing Kaspersky Endpoint Security 12.5 for Linux on devices with Elbrus CPUs. The application offers limited support for Elbrus CPUs.

- Integration with Kaspersky Endpoint Detection and Response Expert (cloud) has been implemented. This cloud solution is designed to protect an IT infrastructure of the organization from advanced cyberthreats, including those that cannot be detected by EPP applications installed on corporate assets. The solution provides comprehensive visibility, correlation, and automation by leveraging a wide range of response tools and data sources, including endpoint assets, network data, and cloud environment data, enabling a unified detection and response process through integrated components and end-to-end workflows within a single interface to enhance the efficiency of security specialists.

  > Integration of Kaspersky Endpoint Security for Linux with the Kaspersky Endpoint Detection and Response Expert (cloud) solution is temporarily not available until this solution is launched, which is planned for late 2026. After that, we expect that integration will become available for this version of Kaspersky Endpoint Security without the need for additional upgrades.

- Password protection of certain actions in the Kaspersky Endpoint Security application. Password protection allows you to restrict actions that users can perform with the Kaspersky Endpoint Security application in accordance with their granted permissions. Restricting access to application settings reduces the risk of unauthorized or unintentional changes to the application.

- The Device Control component has been improved. Now you can export the list of trusted devices to a file and import it from a file.

- Improved BadUSB Attack Prevention component. Now, when you connect a barcode scanner, you can scan a barcode from the screen to authorize the scanner instead of entering an authorization code to unlock the device.

- Improvements to the updatable kernel module (ULKM):

  - Added support for system event interception based on the updatable kernel module (ULKM) for systems with Secure Boot enabled.

  - The application now supports more operating systems on which the updatable kernel module can be used to intercept events.

  - We added support for the updatable kernel module for the Anti-Cryptor and Device Control components.

- We improved the installation process in Astra Linux Special Edition's closed software environment mode Now, if a compatibility pack is installed, the user does not need to manually perform additional actions to start the Kaspersky Endpoint Security application after installing it on a device with the Astra Linux Special Edition operating system.

- Now, when installing the application, you can modify settings of the kesl.ini configuration file using the autoinstall.ini configuration file.

- Improved error diagnostics during application installation and uninstallation:

  - Return codes became more detailed for a clearer understanding of any potential problems.

  - We added new messages about missing dependencies (external libraries, components, utilities, or other programs) required for installation and correct operation of the application.

  - We added new messages about incorrectly configured access permissions of system directories.

  - Kaspersky Security Center displays new and clarified error messages.

  - Now you can ignore package manager errors while installing the application.

- The application now automatically restarts during installation after the first update of the application databases and modules. Now you can configure the application to automatically restart when receiving critical updates after the first 24 hours after installing the application. You can configure an automatic restart of the application on the command line in the general application settings or in the policy properties using the Web Console or the Administration Console.

- Now, when integrating with Detection and Response solutions, you can manage the event cache using the `UseIncreasedXdrEventsCache` setting in the kesl.ini configuration file. There is a trade-off between high performance and RAM footprint.

- Now you can do a fast shutdown of the kesl process when stopping or restarting the application using the `FastShutdown` setting in the kesl.ini configuration file, which helps minimize the downtime of the application on high-load systems and prevent excessive resource consumption.

- Now you can limit the memory consumption of the Behavior Analysis component for processing the event queue using the `ReduceSWMemoryConsumption` setting from the kesl.ini configuration file. The use of this setting may affect the level of protection. Make sure to review the documentation.

- We improved the stability of network access. Now, if the kesl process terminates abnormally, the Watchdog server removes the firewall rules that the application adds when the Web Threat Protection and Network Threat Protection components are started, which lets you avoid losing the internet connection and quickly restore network access on the device.

- Now you can prevent multiple scan tasks from running simultaneously to optimize the application performance. Now, when the option is enabled, if multiple scan tasks are launched simultaneously, they are queued.

- File Threat Protection exclusions can now handle symbolic links. Paths are now converted to final file addresses.

- Now you can enable and configure the dump file directory using the command for managing general application settings, without restarting the application. These dump file configuration settings have been removed from the kesl.ini configuration file.

- A password is now mandatory when integrating with the Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Anti Targeted Attack Platform, and Kaspersky Unified Monitoring and Analysis Platform solutions. Now, when configuring the integration, you must specify a password for the client certificate.

- Now the application can compress traffic when sending telemetry events as part of the Kaspersky Unified Monitoring and Analysis Platform integration, which helps save bandwidth.

- We updated the list of supported operating systems, including support for 64-bit versions of CentOS 5.2, 5.4, 6.4, and 6.6.

- The application interface is available in new languages: Spanish (Mexico) and Portuguese (Brazil).

Changes in older versions

Version 12.4

Kaspersky Embedded Systems Security 12.4 for Linux now has the following new features and improvements:

- Introducing a new functional component, Mail Threat Protection. This component scans the attachments of incoming and outgoing email messages for viruses and other threatening applications.

- Introducing a new functional component, BadUSB Attack Prevention. This component prevents the connection of infected USB devices that imitate a keyboard to a client device.

- The Device Control component has been improved. Now you can grant temporary access to blocked devices upon user request.

- Improvements to the Exploit Prevention component. Now you can configure component-specific scan exclusions for objects.

- Improvements to the updatable kernel module:

  - Now the updatable kernel module lets you optimize file operation interception. Application performance is improved by using a cache of files and processes that do not need to be scanned.

  - Now, by using the updatable kernel module, you can configure global exclusions in a more granular way. If you are using the interception mechanism based on the fanotify technology, the specified mount points are entirely excluded from the interception of file operations. Using the updatable kernel module allows you to exclude specific local or remote directories mounted on the device.

- The EDR (KATA) component, which provides integration with Kaspersky Endpoint Detection and Response (KATA), has been renamed to EDR Expert (on-premises). This component also provides the Kaspersky Endpoint Detection and Response Expert (on-premises) Integration The integration task has been renamed to *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* (KATAEDR, ID: 24).

- Now you can set up integration with Kaspersky Endpoint Detection and Response Expert (on-premises), which is an enterprise cyber security solution that allows defending against most cybersecurity risks and cover the main scenarios of threat spread. Components of Kaspersky Endpoint Detection and Response Expert (on-premises) are deployed on the Open Single Management Platform (OSMP). Integration with Kaspersky Endpoint Detection and Response Expert (on-premises) supports all the capabilities of Kaspersky Endpoint Detection and Response (KATA) Integration, as well as new features:

  - Starting a YARA scan. During a *YARA scan*, Kaspersky Endpoint Security uses YARA files to search for signatures of malicious activity on a device.

  - Collection of forensics, that is, digital data that may be useful when investigating incidents involving cybercrime and data leaks.

  - Sending extended data about events on devices (telemetry) to the telemetry server on the OSMP platform.

- Sending only telemetry with an Indicator of Attack (IOA). You can also now configure custom filters in the Web Console policy.
- Activation of the EDR Expert (on-premises) component, which provides integration with Kaspersky Endpoint Detection and Response Expert (on-premises) and with Kaspersky Endpoint Detection and Response (KATA), by adding a license key.
- Selecting an integration mode in the settings of the *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task on the command line or in policy properties in the Web Console.

- The application can be used in Endpoint Detection and Response Agent mode to support Kaspersky Detection and Response solutions working together with third-party anti-virus solutions on protected devices. In this mode, the device is not protected by the standard protection and control components of Kaspersky Endpoint Security. A third-party application is responsible for the standard protection of the device.
- You can create trace files when the application is started for the first time after installation. Now you can enable trace file creation at the first start of the application in the Web Console, the Administration Console, or in the settings of the initial configuration file.
- The policy management interface in the Web Console has been updated. The structure of sections in the policy has been reworked to help find the functions you need quicker.
- Now you can select the traffic interception mode: the eBPF technology or the iptables utility.
- Now you can select the telemetry source (only eBPF or eBPF plus auditd). For auditd, you can also select an operating mode (exclusive mode or multicast mode).
- Now you can select the mode for sending files and directories to Sandbox for scanning: manual, automatic only, automatic and manual.
- More functionality is available when using the application in Light Agent mode:
  - A system event interception mechanism based on the updatable kernel module is available.
  - The Exploit Prevention functional component is available.
  - Threat detection has been improved.
- Now you can use the Kaspersky Private Security Network (KPSN) directly without using the KSN proxy service on the Administration Server.
- Now you can create out-of-office policies in the Web Console and Administration Console. Out-of-office policies come into effect when a device leaves the organization's network.
- When viewing and exporting the list of mount points in the Web Console or the Administration Console, or when viewing this list on the command line, information about a mount point found in a namespace is now also displayed.
- We improved the alternative mechanism for getting system telemetry in the Behavior Detection component on 64-bit operating systems with kernel versions 4.18 or later with eBPF support, which allows freeing up the resources of the auditd kernel audit subsystem.

- Now you can include the following information in telemetry data when integrating with Kaspersky Managed Detection and Response:
  - Indication of the event occurring in a container
  - ID of the container namespace
  - Container name
- We updated the list of supported operating systems.

Version 12.3

Kaspersky Embedded Systems Security 12.3 for Linux now has the following new features and improvements:

- We added a mechanism for intercepting system events based on the updatable kernel module (not available in Light Agent mode). If the operating system of the device supports fanotify and satisfies other requirements for installing the updatable kernel module, you can configure the application to use the updatable kernel module. Using the updatable kernel module lets you optimize the interception of started processes by Kaspersky Endpoint Security. The updatable kernel module is included in the distribution kit of the application.
- The updatable kernel module improves the functionality of the Anti-Cryptor component (not available in Light Agent mode). The application can now detect more types of ransomware.
- We added a new functional component: Exploit Prevention (not available in Light Agent mode). Exploit Prevention monitors code that exploits vulnerabilities on your device to gain administrative privileges or perform malicious actions.
- The Device Control component has been improved:
  - We added the ability to configure a list of users or user groups where added devices are considered trusted.
  - We added the ability to allow read-only access to storage devices.
  - We also improved user notification through events, adding new events and clarifying and systematizing event texts in plug-ins and on the command line.
- Expanded integration with the Kaspersky Managed Detection and Response solution:
  - Now you can isolate the device from the network.
  - You can quarantine files or restore files from quarantine.
  - You can start or terminate a process.
- We added the ability to activate the MDR component, which provides integration with Kaspersky Managed Detection and Response, by adding a license key.
- The Behavior Detection component has been improved. Now you can enable or disable the exclusion of a process from scanning by MDR and EDR (KATA).
- Now you can configure proxy server exclusions. You can specify which Kaspersky Endpoint Security components must bypass the proxy server, and also create a list of addresses that the proxy server will not be used for. If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the use of a proxy server for connecting to Kaspersky Security Network, the SVM, and the Integration Server is not supported.

- Now you can configure traffic interception exclusions. Now you can use the management plug-ins of the application or command line to specify connections that the application should exclude from traffic interception.

- Now you can temporarily exclude database log files from scanning to optimize the File Threat Protection scan. If a database log file is reused by the same process within 10 minutes of the last scan, the application skips the scan of that log file.

- Now you can enable the merging of exclusion list items in a parent policy and its child policy when inheriting the settings of the parent policy.

- Now you can use the management web plug-in to export and import lists of exclusions in policies and tasks.

- We added the ability to configure the initial configuration settings of the Kaspersky Endpoint Security application in the Kaspersky Security Center Administration Console when creating an installation package or in the properties of an installation package.

- Now you can configure the cancellation of scheduled tasks on a device running on battery power.

- We added the ability to enable or disable the use of a KSN proxy server when Kaspersky Endpoint Security interacts with KSN servers (not available in Light Agent mode). If the use of the KSN proxy server is enabled, Kaspersky Endpoint Security communicates with KSN servers using the KSN Proxy service on the Administration Server. If the use of the KSN proxy server is disabled, Kaspersky Endpoint Security interacts with the KSN servers directly.

- On the command line, you can use a command that displays a list of application functions, information about their status (used or not used), and the Linux technologies that these application features are implemented with.

- We added the ability to display information about the policy and policy profiles in effect on the device in the command line and in the graphical interface.

- Now you can use the command line to install the application on a device that does not have the Perl interpreter installed.

- We improved traffic interception. Now local traffic (traffic between processes on the same device) is not intercepted.

- Now you can pass the necessary settings for sending telemetry when integrated with Kaspersky Managed Detection and Response without having to use the KPSN configuration file. If you are using the Kaspersky Security Network infrastructure solution or if your only tenant is the root tenant, you do not need a KPSN configuration file for integration with Kaspersky Managed Detection and Response.

- Optimized the storage of a large number of events in the application event log. Opening and closing the event database, as well as retrieving events, are now faster operations.

- We improved the graphical interface of the application (if the application is used in Light Agent mode, the graphical interface is not supported):

  - Now you can enable or disable the Web Control component.

  - We reworked the style of the graphical interface (new colors, rounded corners of all windows).

- Changed the names of actions that can be applied to infected objects in the File Threat Protection settings and scan tasks.

- Added an alternative mechanism for getting system telemetry in the Behavior Detection component on 64-bit operating systems (with kernel versions 5.3 or later with eBPF support), which allows freeing up the resources of the auditd kernel audit subsystem. If the operating system satisfies the requirements, the application also uses eBPF automatically in Light Agent mode.

- Dates and times in all application management interfaces (except the command line interface) are displayed in a uniform format conforming to RFC 3339, for example, 2023-12-25 23:55:59.

- We updated the list of supported operating systems.

Version 12.2

Kaspersky Embedded Systems Security 12.2 for Linux now has the following new features and improvements:

- Added support for integration with Kaspersky Network Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform solution, which protects the internal corporate network and allows sending information about events occurring on devices (telemetry) to a Kaspersky Anti Targeted Attack Platform server with the Central Node component (hereinafter also referred to as the NDR server).

- Added support for integration with KATA Sandbox, a component of the Kaspersky Anti Targeted Attack Platform solution, which allows you to analyze and scan objects to detect malicious activity and indicators of targeted attacks on the corporate IT infrastructure using special servers with deployed virtual images of operating systems.

- Added support for integration with Kaspersky Unified Monitoring and Analysis Platform, a comprehensive software solution that combines the following functionality: receiving, processing, and storing information security events; analyzing and correlating incoming data; searching received events, and creating notifications about detection of indicators of information security threats.

- Expanded functionality of integration with Kaspersky Endpoint Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform solution:

  - New object execution prevention functionality.

  - New file quarantining functionality.

  - Expanded information about events on devices (telemetry).

- Expanded Endpoint Detection and Response Optimum integration functionality:

  - New object execution prevention functionality.

  - New file quarantining functionality.

  - Now you can exclude a process from network isolation by process name.

- Now you can use the Cloud Sandbox technology, which allows detecting complex threats on the device. The Kaspersky Endpoint Security application automatically sends detected files to Cloud Sandbox for analysis. Cloud Sandbox runs these files in an isolated environment to detect malicious activity and decides on the reputation of these files.

- Now you can view statistics for the most frequently scanned files and applications, as well as a list of mount points detected on the protected device. To improve performance, you can now exclude the files most frequently scanned by the File Threat Protection component, the paths to applications most frequently scanned by the Behavior Detection component, and the mount points detected on the device.

- Now you can collect application performance metrics that can help analyze the impact of Kaspersky Endpoint Security on operating system performance.

- Improved Firewall Management component. Now you can specify multiple IP addresses or IP address ranges for a network packet rule.

- New mechanism for tracking operating system freezes. This mechanism checks for freezes of some system functions, one such function being the execve function. Every three seconds, the wdserver Watchdog server process starts another wdserver process, in which it calls these system functions (an execve function call starts at least one additional wdserver process). If wdserver detects an unresponsive system function, the Watchdog server overload restarts the kesl process.

- Now you can configure the display of pop-up notifications when managing the graphical user interface of the application. Now you can enable or disable the display of pop-up notifications in the GUI using the Web Console, Administration Console, or command line.

- Improved command line options for task scheduling. Now you can configure a task to be stopped when it reaches the maximum allowed execution time.

- Changed the status of the "padlock" attribute when creating a Kaspersky Security Center policy profile. Now, when creating a profile, all "padlocks" are open by default, which means that by default, profile settings do not override the settings of the "base" policy.

- Added an alternative mechanism for getting system telemetry on 64-bit operating systems (with kernel versions 5.3 or later with eBPF with BTF support), which allows freeing up the resources of the auditd kernel audit subsystem. The application will work with eBPF automatically if the operating system meets the specified requirements.

- Dates and times in all management plug-ins are displayed in a uniform format conforming to RFC 3339, for example, 2023-12-25 23:55:59.

- We updated the list of supported operating systems.

Version 12.1

Kaspersky Embedded Systems Security 12.1 for Linux now has the following new features and improvements:

- Now you can set up integration with Kaspersky Endpoint Detection and Response Optimum, which protects the organization's IT infrastructure from threats such as exploits, ransomware, fileless attacks and attackers' use of legitimate system tools to harm devices or data.

- Now you can add two active license key to the application: the main key for activating the application and an additional key for activating the Kaspersky Endpoint Detection and Response Optimum functionality. The additional key is required if your main license does not include the Kaspersky Endpoint Detection and Response Optimum functionality.

- Added a new *Web Control* component, which controls user access to web resources. This allows you to reduce traffic consumption and reduce inappropriate use of work time. If a user tries to open a website to which access is restricted by Web Control, Kaspersky Endpoint Security blocks access or displays a warning.

- The newly added Kaspersky Endpoint Security stability monitoring functionality allows you to track the number of times the application terminates abnormally and notify the administrator about the unstable operation of the application.

- The procedure for installing Kaspersky Endpoint Security using the Kaspersky Security Center Web Console has been improved: in the properties of the application installation package, you can now specify initial configuration settings that were previously available only in the autoinstall.ini configuration file.

- More application settings can be specified using the Kaspersky Security Center Web Console and the Kaspersky Security Center Administration Console: you can edit settings that previously could be set only by editing the kesl.ini configuration file.
- Now you can enable or disable global exclusions and File Threat Protection exclusions when running scan tasks.
- Now you can set up integration with Kaspersky Symphony XDR: if the Kaspersky Endpoint Security application is being used in standard mode, the application can perform the "Start Malware Scan" and "Database update" response actions.
- Now you can send information about all devices installed on or connected to client devices (including those installed and connected previously but currently disconnected) to the Administration Server when the application is managed using Kaspersky Security Center.
- Traffic interception rules have been improved to support the interaction of containers on the same network.
- We updated the list of supported operating systems.

Fixed issues

The table below lists all issues discovered in previous versions of Kaspersky Endpoint Security and fixed in the current version.

List of issues fixed in version 12.5

Identifier	Description
10306343	When checking the status of a current license key, notifications about the removal and installation of a license key were generated erroneously.
10295949	The settings specified in the current policy profile for the Device Control component were not applied. As a result, the component continued to work with the settings specified in the policy.
10171454	If the first update source specified in the settings was unavailable, a message about an update problem was displayed erroneously.
10109293	If the iptables network traffic interception mode was selected (`NetInterceptorMode=UseIPTables`), traffic from applications opening network sockets bound to a specific network interface was processed incorrectly.
10024219	The Kaspersky Security Center Administration Console incorrectly displayed the status of the updatable kernel module on managed devices.
9995631	The limitation on resident RAM usage by the application (the `MaxMemory` setting) worked incorrectly on systems without a swap partition. Now, when the set limit is reached, Kaspersky Endpoint Security restarts.
9937329	*Device connected* and *Device disconnected* were generated erroneously on systems with the Device Control (Device_Control) task disabled.
9934846	The application would not start on high-load systems. The timeout for the application's connection to the Watchdog server has been increased.
9846405	*Object not processed* events were generated erroneously on systems with a configured EFI bootloader.
9815051	Previously established network connections could hang when running the Web Threat Protection (Web_Threat_Protection) and Network Threat Protection (Network_Threat_Protection) tasks on managed devices in eBPF network traffic interception mode (`NetInterceptorMode=UseEBPF`). Such connections are now terminated when an attempt to transmit data is made.
9807202	On some ROSA operating systems, problems were encountered with installation when using the mkfs.ext2 utility.
9704644	The device status was displayed incorrectly when the application was used in the EDR agent mode. Changed the value of the device protection status when the application is being used in EDR Agent mode.

Identifier	Description
9643969	In some cases, when using network traffic interception in eBPF mode, an issue may arise with network connectivity between Scylla hosts.
9633030	The Execution prevention for objects (EDR Expert (on-premises)) task would run when the **Enable execution prevention for objects** check box was cleared in the policy.
9627894	The network traffic interception mode based on eBPF technology worked incorrectly on operating systems with disabled IPv6.
9606448	Issue occurred with activating the application using the Kaspersky Security Center Administration Server as a proxy server for access to Kaspersky activation servers (when the **Use Kaspersky Security Center as proxy server for activation** check box was selected in the policy).
9508605	When Kaspersky Endpoint Detection and Response Expert integration was enabled, the application used a large amount of memory on systems with a container environment.
9456741	The application crashed due to the inability to determine the file interpreter when intercepting the start of a new process.

List of issues fixed in version 6.1 of the web plug-in

Identifier	Description
9558745	The **Show pop-up notifications in the graphical user interface** setting for configuring the display of notifications in the graphical interface of Kaspersky Endpoint Security was not displayed in the policy properties (**Application settings** → **General Settings** → **Event settings** → **Advanced settings**).
9622658	When adding exclusions from Malware Scan by object hash, such exclusions were not saved.
9798821	When adding an individual website to a Web Control rule, policy changes were not saved.
9990129	An irrelevant **Comment** field was displayed in the form for adding a trusted application.
9977884	An irrelevant **Security level** toggle switch was displayed in the settings of the Mail Threat Protection component.
9944635	The name of the **Scan email databases** flags was duplicated. Correct names are now displayed: **Scan email databases** and **Scan email format files**.
10010439	When creating Web Control rules, the user assigned to the rule from the Active Directory list was added incorrectly.
10218308	The Kaspersky Security Network mode was reset when the policy settings were changed.

Hardware and software requirements

Minimum hardware requirements

For application installation

- CPU with AMD64 architecture, 2 GHz or more, two or more cores, and support for the SSE2 instruction set.
- Swap space of at least 1 GB
- RAM:
  - For 64-bit operating systems: 2 GB of RAM available for the application
  - For 32-bit operating systems: 1 GB of RAM available for the application
- 4 GB of free hard disk space for installation of the application and storage of temporary and log files

Additional disk space is required to store trace files and application memory dump files.

When scanning archives and compound objects with `ScanArchived=Yes` and/or `ScanSfxArchived=Yes` (by default, these are set to `Yes` for scan tasks and `No` for File Threat Protection), File Threat Protection and scan tasks require additional disk space depending on the type and unpacked size of such objects.

We recommend making sure there is enough free space in the /tmp directory for scanning archives and compound objects. You can also limit the size (in the archived state) of archives that can be scanned by specifying the `SizeLimit` setting for each task.

To install the graphical user interface

- A monitor capable of displaying windows 1000 pixels wide by 600 pixels tall. If screen scaling is applied, these dimensions are also scaled.

Minimum hardware requirements for the Arm architecture

For application installation

- Armv8.2-A Kunpeng 920 or Armv8-A Baikal-M (BE-M1000) CPU or m-TrusT Terminal platform
- Swap partition of at least 1 GB
- 2 GB of RAM available to the application
- 3 GB of free hard disk space for installation of the application and storage of temporary and log files

  Additional disk space is required to store trace files and application memory dump files.

  When scanning archives and compound objects with `ScanArchived=Yes` and/or `ScanSfxArchived=Yes` (by default, these are set to `Yes` for scan tasks and `No` for File Threat Protection), File Threat Protection and scan tasks require additional disk space depending on the type and unpacked size of such objects.

  We recommend making sure there is enough free space in the /tmp directory for scanning archives and compound objects. You can also limit the size (in the archived state) of archives that can be scanned by specifying the `SizeLimit` setting for each task.

To install the graphical user interface

- A monitor capable of displaying windows 1000 pixels wide by 600 pixels tall. If screen scaling is applied, these dimensions are also scaled.

Minimum hardware requirements for the Elbrus (E2K) architecture

For application installation

- CPU v3: Elbrus-4S; v4: Elbrus-8S or Elbrus-1S+
- Swap partition of at least 2 GB
- 2 GB of RAM available to the application
- 2 GB of free hard disk space for installation of the application and storage of temporary and log files

To install the graphical user interface

- A monitor capable of displaying windows 1000 pixels wide by 600 pixels tall. If screen scaling is applied, these dimensions are also scaled.

Software requirements

To install Kaspersky Endpoint Security, one of the operating systems listed in the table must be installed on the device:

This article lists the software versions on which the application has been tested and for which it is guaranteed to work correctly. The application may also work with other software versions, but those configurations have not undergone a full testing cycle and are not included in the list of guaranteed-supported versions.

Due to technical limitations of fanotify, the application does not support the following file systems: autofs, binfmt_misc, cgroup, configfs, debugfs, devpts, devtmpfs, gfs2, gvfs, hugetlbfs, mqueue, nfsd, proc, parsecfs, pipefs, pstore, usbfs, rpc_pipefs, securityfs, selinuxfs, sysfs, tracefs.

File Threat Protection for mount points via the FUSE technology is limited without additional steps that the administrator of the operating system must complete. You can add the user_allow_other settings to the /etc/fuse.conf file and the allow_root mount option for each mount point, allowing the application to monitor file events at those mount points.

64-bit operating systems	64-bit operating systems for the Arm architecture	64-bit operating systems for the Elbrus (E2K) architecture	32-bit operating systems
• AlmaLinux OS 8.6, 8.7, 8.8, 8.9. • AlmaLinux OS 9.4, 9.5, 9.6. • AlterOS® 2025. • Amazon™ Linux 2023. • Astra Linux Common Edition 2.12. • Astra Linux Special Edition RUSB.10015-01 (operational update 1.5, 1.6, 1.7, 1.8). • Astra Linux Special Edition RUSB.10015-03 (operational update 7.6). • Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6). • Astra Linux Special Edition RUSB.10015-17 (operational update 1.7.3) • Astra Linux Special Edition RUSB.10015-37 (operational update 7.7). The Astra Linux operating system in the "Mobile" mode is only supported in desktop mode. • CentOS 5.2, 5.4, 6.4, 6.6, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. In the Kaspersky Endpoint Security Cloud solution, the application does not support running on CentOS 5.2, 5.4, 6.4, 6.6 devices. In Kaspersky Security Center Cloud Console, the application does not support running on CentOS 5.2, 5.4, 6.4, 6.6 devices. • CentOS Stream 8, 9, 10. • Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13. • Debian GNU/Linux 13.1, 13.2, 13.3. • EMIAS 1.0. • EulerOS 2.0 SP10. • Fedora Linux 41. • Kylin Desktop OS V10 SP1. • Linux Mint 21.3. • Linux Mint 22.2. • Mostech 12 release 2021.1. • openSUSE Leap 15.6. • Oracle Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. • Oracle Linux 8.5, 8.6, 8.7, 8.8, 8.9. • Oracle Linux 9.4, 9.5, 9.6. • Red Hat Enterprise Linux 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9. • Red Hat Enterprise Linux 8.5, 8.6, 8.7, 8.8, 8.9, 8.10. • Red Hat Enterprise Linux 9.4, 9.5, 9.6. • Red Hat Enterprise Linux 10.0, 10.1. • Rocky Linux 8.6, 8.7, 8.8, 8.9. • Rocky Linux 9.4, 9.5, 9.6. • SberLinux 8.10, 9.1, 9.5, 9.6, 9.7. • SberOS 3.4.0, 3.5.0, 3.6.1. • SUSE Linux Enterprise Server 12.5, 12.6, 12.7. • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7. • Ubuntu® 24.04 LTS. • Ubuntu 26.04 LTS. • ALT Education 10, 11. • ALT Workstation 11. • ALT Server 11. • ALT SP Workstation release 10. • ALT SP Server release 10.	• Astra Linux Special Edition RUSB.10152-02 (operational update 4.7). • CentOS Stream 9. • EulerOS 2.0 SP10. • SUSE Linux Enterprise Server 15.4, 15.5, 15.6, 15.7. • Ubuntu 26.04 LTS. • ALT Workstation 11.2 • ALT Server 11.1. • ALT SP Workstation release 10. • ALT SP Server release 10. • RED OS 8.0.	• OS Elbrus 9.3.6. • Astra Linux Special Edition RUSB.10015-16 (release 2) (operational update 8.1). • Astra Linux Special Edition RUSB.10265-01 (operational update 8.1). • ALT SP Workstation release 8, 10. • ALT SP Server release 8, 10.	• Debian GNU/Linux 12.8, 12.9, 12.10, 12.11, 12.12, 12.13.

64-bit operating systems	64-bit operating systems for the Arm architecture	64-bit operating systems for the Elbrus (E2K) architecture	32-bit operating systems
• Atlant, Alcyone build, version 2022.02. • GosLinux 7.2. • M OS 12 Server release 2021.1. • Mos OS 15.5 Arbat. • MSVSphere 9.5 Workstation. • MSVSphere 9.5 Server. • MES OS 12 Panel release 2025. • MES OS 12 Desktop release 2025. • OSnova 3.1. • RED OS® 7.3. • RED OS 8.0. • ROSA "Cobalt" 7.9 Workstation. • ROSA "Cobalt" 7.9 Server. • ROSA "Chrome" 12 Workstation. • ROSA "Chrome" 12 Server. • SintezM-Client 8.6. • SintezM-Server 8.6.			

Additional software and hardware requirements for Light Agent mode

Kaspersky Endpoint Security can be used as a Light Agent as part of Kaspersky Security for Virtualization Light Agent 6.5. You can view the virtual infrastructure requirements of the application in Light Agent mode in Kaspersky Security for Virtualization Light Agent Help.

Virtual machines

The software and hardware requirements of Kaspersky Endpoint Security apply with the following limitations to virtual machines with Kaspersky Endpoint Security in Light Agent mode:

- A virtualized network interface with a bandwidth of 100 Mbps is necessary
- On Arm devices, Kaspersky Endpoint Security in Light Agent mode is not supported.
- The application in Light Agent mode is not supported in the Astra Linux Special Edition operating systems in the mandatory access control mode and closed software environment mode.

The BIOS on a virtual machine must support the SMBIOS specification version 2.1 or later.

Depending on your virtual infrastructure, virtual machines must have the following installed:

- In a Microsoft Hyper-V infrastructure, the Integration Services package.
- In a VMware vSphere infrastructure, the VMware Tools package.
- In a XenServer infrastructure, the XenTools software.
- In a HUAWEI FusionSphere infrastructure, the HUAWEI Tools package.
- In a KVM (Kernel-based Virtual Machine) infrastructure, QEMU Guest Agent.

Supported terminal server types

- Astra Linux 3.0.5 terminal server.

Distribution kit

The Kaspersky Endpoint Security distribution kit includes the following files:

Main application files

- For processors with 32-bit operating system:
  `kesl-12.5.0-<build number>.i386.rpm`
  `kesl_12.5.0-<build number>_i386.deb`
- For processors with 64-bit operating system:
  `kesl-12.5.0-<build number>.x86_64.rpm`
  `kesl_12.5.0-<build number>_amd64.deb`
- For Arm® processors, 64-bit operating system:
  `kesl-12.5.0-<build number>.aarch64.rpm`
  `kesl_12.5.0-<build number>_arm64.deb`
- For Elbrus CPU:
  `kesl-12.5.0-<build number>.e2k.rpm`
  `kesl_12.5.0-<build number>_e2k.deb`

Graphical interface of the application

- For processors with 32-bit operating system:
  `kesl-gui-12.5.0-<build number>.i386.rpm`
  `kesl-gui_12.5.0-<build number>_i386.deb`
- For processors with 64-bit operating system:
  `kesl-gui-12.5.0-<build number>.x86_64.rpm`
  `kesl-gui_12.5.0-<build number>_amd64.deb`
- For Arm® processors, 64-bit operating system:
  `kesl-gui-12.5.0-<build number>.aarch64.rpm`
  `kesl-gui_12.5.0-<build number>_arm64.deb`
- For Elbrus CPU:
  `kesl-gui-12.5.0-<build number>.e2k.rpm`
  `kesl-gui_12.5.0-<build number>_e2k.deb`

To install the Kaspersky Endpoint Security application on operating systems with limited support (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), select the distribution package marked `OLD`.

Archive for remote installation of the application using Kaspersky Security Center

`kesl-12.5.0.<build number>.zip`

The archive also contains the texts of user agreements.

Texts of user agreements

- `ksn_license.<language ID>` contains the text of the Kaspersky Security Network Statement.
- `license.<language ID>` contains the text of the End User License Agreement. The End User License Agreement specifies the terms for using the application.

Kaspersky Security Center Network Agent is not included in the distribution kit. You can download it on the application download page in the **Kaspersky Security Center** section.

Compatibility with other applications

Supported versions of Kaspersky Security Center

Depending on the mode of Kaspersky Endpoint Security, you can manage the application using the Kaspersky Security Center versions listed in the table.

Mode	Kaspersky Security Center version
Kaspersky Endpoint Security in Standard mode	Kaspersky Security Center Windows 14.2, 15.1. Management via the Administration Console using the MMC administration plug-in, and via the Kaspersky Security Center Web Console using the web administration plug-in. Kaspersky Security Center Linux 15.1, 15.2, 15.3, 15.4, 16.0, 16.1, 16.2, 16.3. Management via the Kaspersky Security Center Web Console using the web administration plug-in.
Kaspersky Endpoint Security in Standard mode with the Endpoint Detection and Response Optimum component	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.
Kaspersky Endpoint Security in Light Agent mode	Kaspersky Security Center Windows 15.1. Kaspersky Security Center Linux 16.1, 16.2, 16.3.
Kaspersky Endpoint Security in EDR Agent mode	Kaspersky Security Center Windows 14.2, 15.1. Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2, 16.3.

Supported version of Kaspersky Security for Virtualization Light Agent

Kaspersky Endpoint Security can be used as a Light Agent as part of Kaspersky Security for Virtualization Light Agent 6.5.

Supported versions of solutions on KATA and OSMP platforms

Kaspersky Endpoint Security is compatible with solutions based on the Kaspersky Anti Targeted Attack Platform and the Kaspersky Endpoint Detection and Response Expert (on-premises) solution of the following versions:

- Kaspersky Anti Targeted Attack Platform 6.0, 6.1, 7.0, 7.1 (Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), including scenarios for sending files to Sandbox for scanning).
- Kaspersky Anti Targeted Attack Platform 8.0 (Kaspersky Network Detection and Response (KATA), including scenarios for sending files to Sandbox for scanning).

  For more details about the Kaspersky Anti Targeted Attack Platform solution, please refer to the Kaspersky Anti Targeted Attack Platform Help.
- Kaspersky Endpoint Detection and Response Expert (on-premises) 8.0, 8.1 on the Open Single Management Platform (hereinafter also referred to as OSMP), including scenarios for sending files to Sandbox for scanning.

  For more information about Kaspersky Endpoint Detection and Response Expert (on-premises), see the Kaspersky Endpoint Detection and Response Expert (on premise) Help.

Supported versions of the Network Agent for integration with Kaspersky Endpoint Detection and Response Expert (cloud)

To integrate the application with Kaspersky Endpoint Detection and Response Expert (cloud), you need a Network Agent for Kaspersky Security Center Cloud Console of certain versions described in the Kaspersky Security Center Cloud Console Help.

Compatibility with third-party solutions

Kaspersky Endpoint Security in EDR Agent mode can work together with the Dr. Web anti-virus application.

Comparison of functionality across Kaspersky solutions

Kaspersky Endpoint Security is included in many Kaspersky multiplatform solutions. The available application functionality is determined by the solution that you purchased from a service provider in your region.

Feature	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Optimum	Kaspersky Next MXDR Optimum	Kaspersky Next EDR Expert	Kaspersky Next XDR Expert	Kaspersky Hybrid Cloud Security, Desktop	Kaspersky Hybrid Cloud Security Enterprise Desktop/CPU/Server	Kaspe Clou Core/
File Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓	
Mail Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓	

Web Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓	
Network Threat Protection	✓	✓	✓	✓	✓	✓	✓	✓	
Firewall Management	✓	✓	✓	✓	✓	✓	✓	✓	
Behavior Detection	✓	✓	✓	✓	✓	✓	✓	✓	
BadUSB Attack Prevention	–	✓	✓	✓	✓	✓	✓	✓	
Device Control	✓	✓	✓	✓	✓	✓	✓	✓	
Removable Drives Scan	✓	✓	✓	✓	✓	✓	✓	✓	
Anti-Cryptor (for shared folders)	✓	✓	✓	–	✓	✓	–	✓	
Container Scan	–	–	–	–	–	✓	–	✓	
Application Control	✓	✓	✓	✓	✓	✓	✓	✓	
Web Control	✓	✓	✓	✓	✓	✓	✓	✓	
Integration with Kaspersky Unified Monitoring and Analysis Platform	–	–	–	–	–	✓	–	–	
Integration with Kaspersky Endpoint Detection and Response Expert (cloud)	–	–	–	–	✓	✓	–	–	
Integration with Kaspersky Endpoint Detection and Response Expert (on-premises)	–	–	–	–	✓	✓	–	–	
Kaspersky Endpoint Detection and Response Optimum	✓	✓	✓	✓	–	–	–	–	
Integration with Kaspersky Managed Detection and Response	–	–	–	✓	–	–	–	–	

Deployment and initial configuration

You can follow this scenario to deploy the Kaspersky Endpoint Security application and prepare it for use.

1 Selecting the application usage mode

After you have purchased a Kaspersky solution on the official Kaspersky website or from one of our partners, you will receive a message at the email address that you specified during the purchase. This message will contain an activation code and information on how to get a key file. You may need a key file if your organization does not support online activation of the application using a code.

Your choice of solution determines the modes in which you can use the application:

- If you have a Kaspersky Endpoint Security license, you can use the application in Standard mode.
- If you have a Kaspersky Security for Virtualization Light Agent license, you can use the application in Light Agent mode.
- If you have a Kaspersky Endpoint Detection and Response Expert (on-premises) license, you can use the application in EDR agent mode.

The application deployment depends on the selected mode.

After Kaspersky Endpoint Security is installed, you cannot change the application usage mode.

2 Preparing the environment

Complete the necessary preparatory actions depending on your infrastructure.

3 Selecting the system event interception mechanism

If the operating system of your device supports fanotify, during installation, you can select which mechanism to use to intercept system events.

4 Preparing distribution packages

Download files required to install the application. Which files you need depends on the operating system of the protected device and the application deployment method.

5 Preparatory actions in Kaspersky Security Center

Perform preparatory actions in Kaspersky Security Center. We recommend using Kaspersky Security Center for centralized management of your organization's protection. Kaspersky Security Center is also required if you will be using Kaspersky Endpoint Security in EDR agent mode or in Light Agent mode.

6 Installing the application

Install the application on devices using the method that suits the needs of your organization:

- Installing the application using Kaspersky Security Center
- Installing the application using the command line

7 Additional configuration steps after installation in certain operating systems

Some Linux operating systems need additional configuration after installation of Kaspersky Endpoint Security.

Modes and deployment schemes

Kaspersky Endpoint Security is part of many Kaspersky solutions. Your choice of solution determines the application's operating mode and deployment scheme.

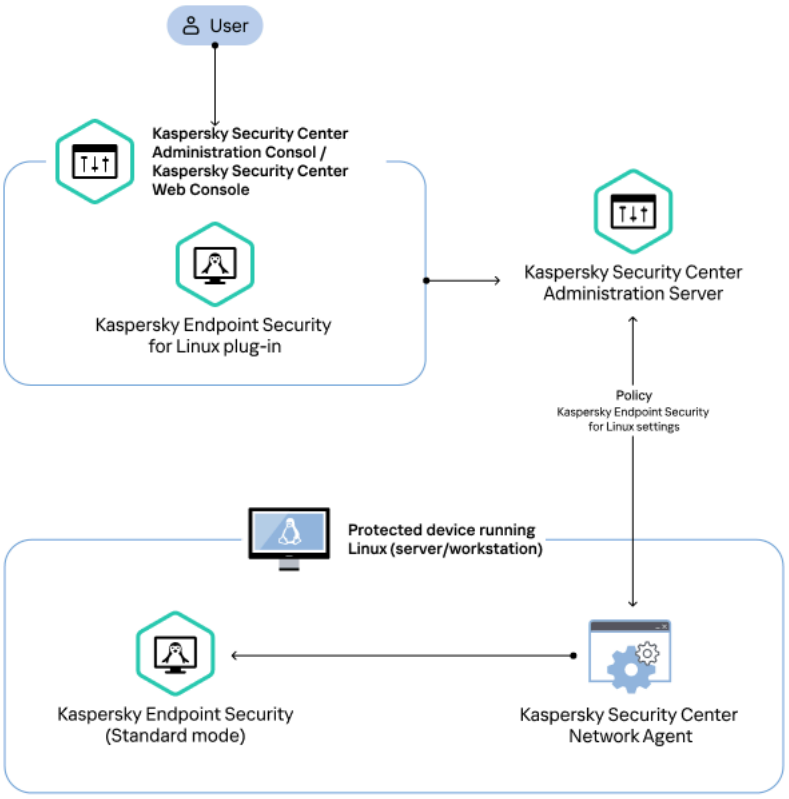
Standard mode

The default mode of the application. Kaspersky Endpoint Security provides comprehensive protection against various types of threats, network attacks and fraud for Linux workstations and servers.

In this mode, the application uses device protection and control components such as File Threat Protection or Behavior Detection and also built-in agents to protect against advanced threats and targeted attacks.

You can install the application in this mode as part of Kaspersky EPP (Endpoint Protection Platform) solutions. For example, Kaspersky Endpoint Security in Standard mode is part of the Kaspersky Endpoint Security for Business.

The mainstream deployment scheme of Kaspersky Endpoint Security is centralized deployment via Kaspersky Security Center. On each protected device, you need to install Kaspersky Endpoint Security and the Kaspersky Security Center Network Agent component. This component connects devices to the Kaspersky Security Center Administration Server and allows managing devices using Kaspersky Security Center.



Deployment scheme for Kaspersky Endpoint Security in Standard mode

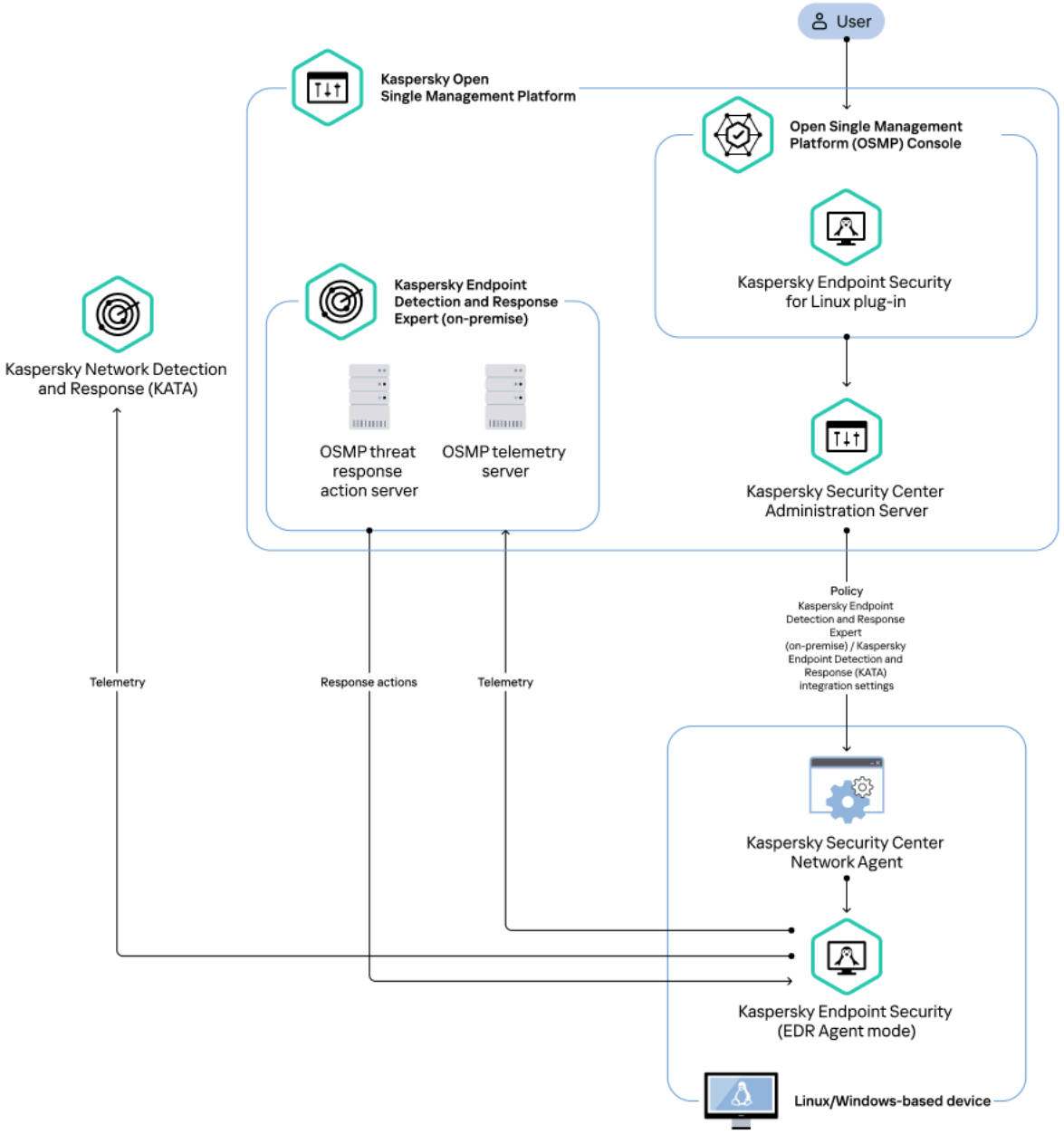
Endpoint Detection and Response Agent (EDR Agent) mode

This mode allows deploying Kaspersky Detection and Response solutions together with third-party anti-virus solutions. Detection and Response solutions include:

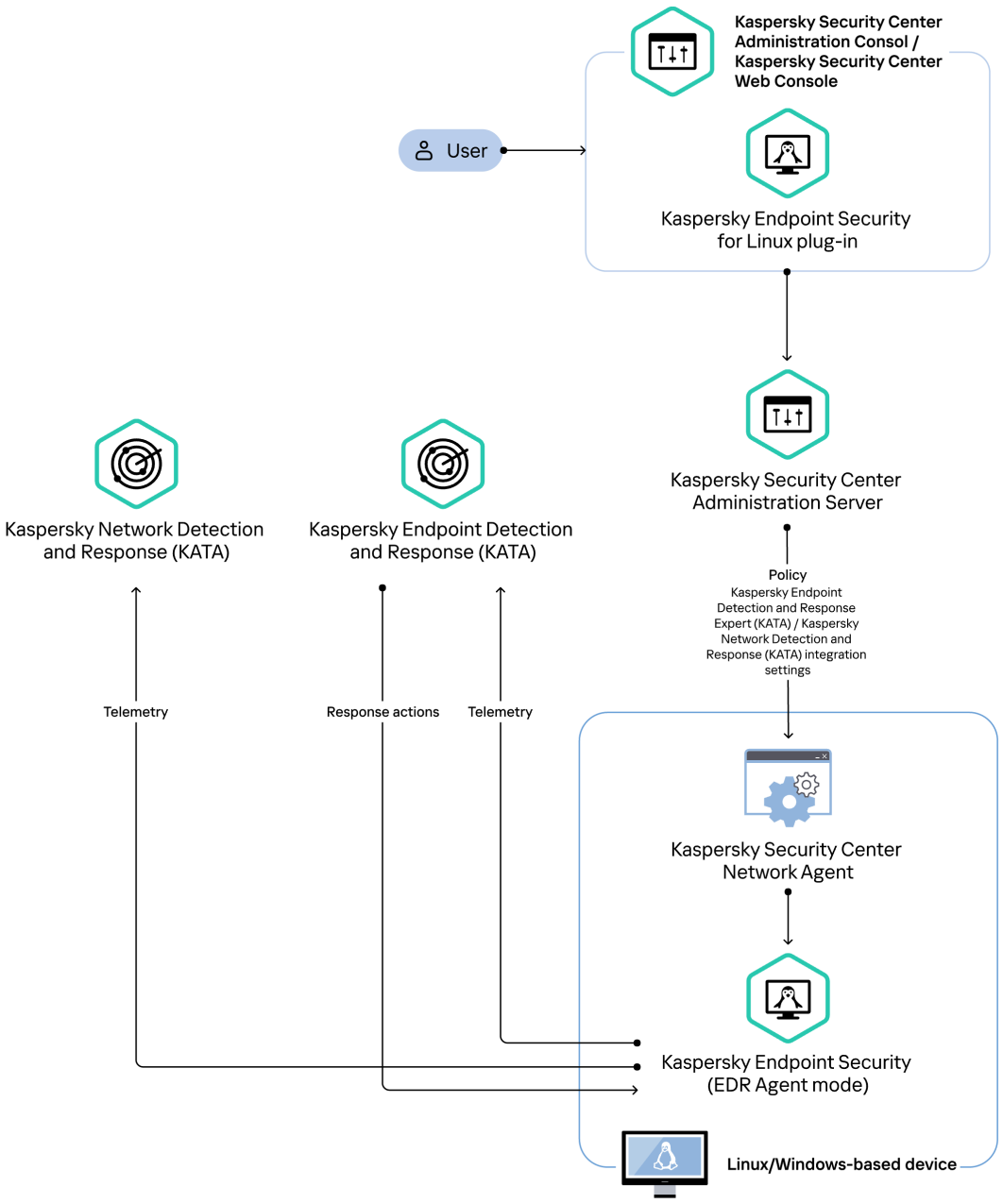
- Kaspersky Endpoint Detection and Response Expert (on-premises) on the Open Single Management Platform (hereinafter also referred to as "OSMP").
- Kaspersky Endpoint Detection and Response and Kaspersky Network Detection and Response on the Kaspersky Anti Targeted Attack Platform (hereinafter also referred to as "KATA").

In EDR Agent mode, protection and control components such as File Threat Protection or Web Threat Protection are not available. A third-party anti-virus application protects the device. The EDR agent continuously monitors processes running on these devices, network connections being opened and files being modified, and interacts with Detection and Response solutions to protect against advanced threats and targeted attacks.

For Kaspersky Endpoint Security to operate in EDR Agent mode, you must deploy the appropriate infrastructure; for more information, see the Help section for the Detection and Response solution you selected. Learn more about the special aspects of the EDR Agent mode in the Known issues and limitations article.



Deployment scheme for Kaspersky Endpoint Security in EDR Agent mode together with Kaspersky Endpoint Detection and Response Expert (on-premises)



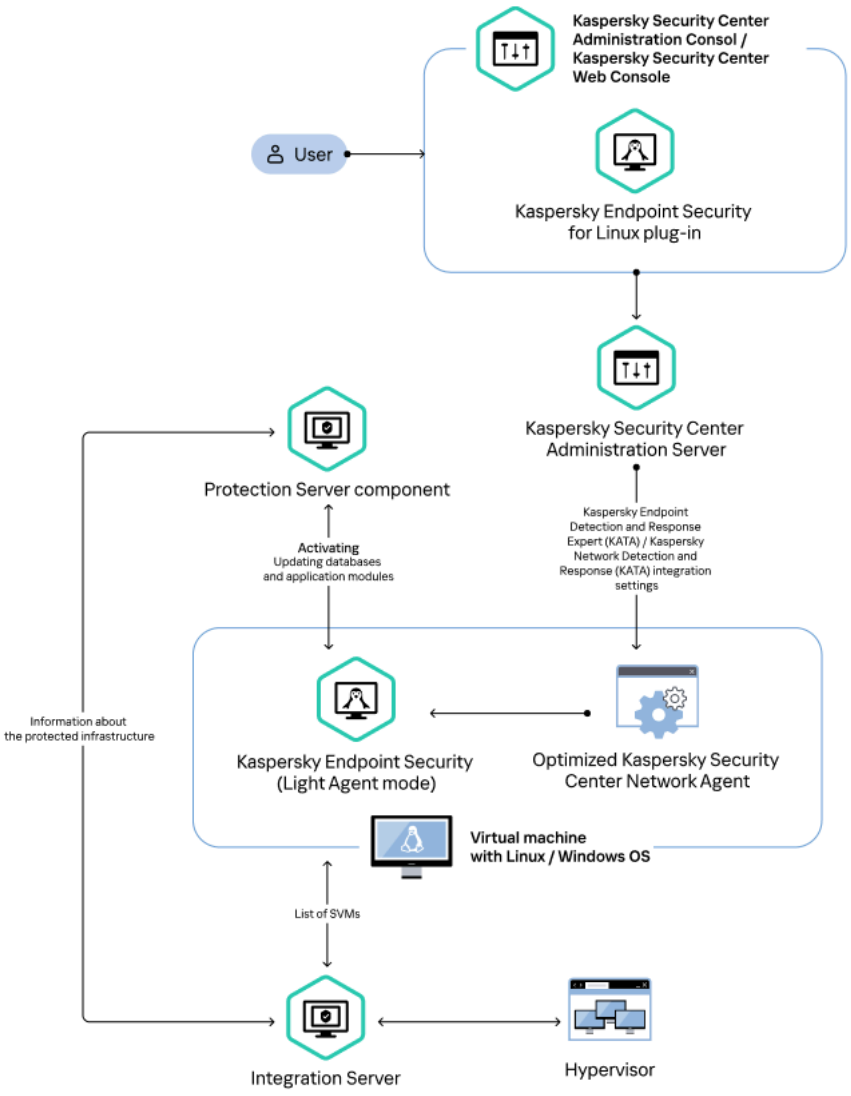
Deployment scheme for Kaspersky Endpoint Security in EDR Agent mode together with Kaspersky Endpoint Detection and Response and Kaspersky Network Detection and Response

Light Agent mode

Kaspersky Endpoint Security in Light Agent mode is part of the Kaspersky Security for Virtualization Light Agent solution for protecting virtual machines running Linux guest operating systems.

The same protection and control components are available in this mode as in Standard mode. The difference is that objects are scanned for viruses and other malware, license keys are added, and databases and modules are updated by a special solution component installed on a separate virtual machine, SVM (Secure Virtual Machine). This helps relieve the hypervisor because the application in Light Agent mode uses the resources of the SVM to protect the infrastructure instead of resources of virtual machines.

For Kaspersky Endpoint Security to operate in Light Agent mode, you must deploy the appropriate infrastructure; for more information, see the Kaspersky Security for Virtualization Light Agent Help. Learn more about the special aspects of the Light Agent mode in the Known issues and limitations article.



Deployment scheme for Kaspersky Endpoint Security in Light Agent mode

After selecting the application mode, you can go back to the deployment scenario and continue from the Preparing the environment step.

Preparing the environment for installing the application

Preparing the infrastructure

Kaspersky Security Center

If you intend to manage the application centrally using Kaspersky Security Center, install Kaspersky Security Center in your infrastructure. If you have already installed Kaspersky Security Center Windows and are planning to migrate to Kaspersky Security Center Linux, follow these instructions: Migrating data to Kaspersky Security Center Linux.

Kaspersky Endpoint Security in EDR Agent mode

For Kaspersky Endpoint Security to operate in EDR Agent mode, you must deploy the appropriate infrastructure; for more information, see the Help section for the Detection and Response solution you selected.

Kaspersky Endpoint Security in Light Agent mode

For Kaspersky Endpoint Security to run in Light Agent mode, you need to deploy the Kaspersky Security for Virtualization Light Agent solution:

1. Install the components of the Kaspersky Security for Virtualization Light Agent solution, namely the Integration Server and the Protection Server.

2. Prepare the Protection Server for operation by activating the solution and configuring database updates for the Protection Server and Light Agents.

   For more details about the installation and configuration of solution components, refer to the Help for Kaspersky Security for Virtualization Light Agent.

3. Make sure that the virtual machines that you want to protect satisfy the requirements for Light Agent mode.

4. Make sure that the settings of network equipment or software that monitor traffic between virtual machines allow network traffic to pass through the ports that are used for interaction between Kaspersky Endpoint Security in Light Agent mode and other components of Kaspersky Hybrid Cloud Security for Virtualization Light Agent. The ports used by the Light Agent are listed in the Kaspersky Security for Virtual Environment Light Agent Help.

The Light Agent mode of Kaspersky Endpoint Security is not supported on devices based on the Arm architecture and with an Elbrus CPU.

Preparing the device for installation

- Check if your device meets the hardware and software requirements of the application.

- If you want to install Kaspersky Endpoint Security in Standard mode or in Light Agent mode, make sure that no third-party anti-virus software is installed on your device. In EDR agent mode, Kaspersky Endpoint Security can work together with the Dr. application. Web anti-virus application.

- Make sure that Kaspersky Endpoint Agent for Linux is not installed on your device. If Kaspersky Endpoint Agent for Linux is installed, uninstall it.

- Make sure the iptables utility is installed on your device. The application requires the iptables utility to intercept network traffic.

- Make sure that root is the owner of the following directories and that only the owner has write access: /var, /var/opt, /opt, /usr/bin, /usr/lib, /usr/lib64. This is required for the application to start and work correctly.

- When the application is running, the operating system may use significantly more file descriptors. Make sure that the limit on the number of descriptors is sufficiently high. To check the limit, run the command `cat /proc/sys/fs/file-max`. In general, we recommend disabling the limit by specifying `fs.file-max=9223372036854775807` in the /etc/sysctl.conf file. After making this change, restart the operating system.

- Make sure that `kernel.yama.ptrace_scope=0` in the operating system. Other values of the `kernel.yama.ptrace_scope` parameter may affect the operation of the Kaspersky Endpoint Security application; for more details, see the Known issues and limitations section.

Additionally, to install the graphical interface of the application:

- The version of the kesl-gui package that you are installing must match the version of your kesl package.

- For the graphical interface of Kaspersky Endpoint Security to work correctly, the Zenity utility must be installed in your operating system.

- If your device has access to repositories of the package manager, all necessary dependencies are installed automatically during the installation of the graphical installing the graphical interface of the application. If the device is in a private segment and does not have access to the repositories of the package manager:

  1. Check the list of dependencies on a reference device (libice6, libsm6, zlib1g, kesl).

  2. Do one of the following:

     - Before installing the graphical interface, download the packages to all devices and then install them using the package manager.

     - Make sure that packages are downloaded to devices during the installation of the graphical interface.

Additionally for MMC plug-in support

If you intend to use the Kaspersky Security Center Administration Console to manage the application, install Microsoft® Visual C++® 2015 Redistributable Update 3 RC on the device where the Administration Server is installed (see https://www.microsoft.com/en-us/download/details.aspx?id=52685). This is necessary for the Kaspersky Endpoint Security MMC management plug-in to work.

Additionally for certain operating systems

Astra Linux in closed software environment mode

Installing the compatibility pack

You need to install the compatibility pack in the following cases:

- Before installing the application in closed software environment mode.
- With the application already installed, when switching the operating system to closed software environment mode.

Install package

```
apt install astra-digsig-oldkeys
```

This will allow running the application in Astra Linux Special Edition operating systems (updates 4.7 for the Arm architecture, 1.6, 1.7, and 1.8) in the closed software environment mode.

Re-allowing ptrace

By default, Astra Linux operating systems block ptrace (Disable ptrace capability), which may affect the operation of Kaspersky Endpoint Security. For Kaspersky Endpoint Security to work correctly, we recommend unblocking ptrace when installing Astra Linux. If Astra Linux is already installed, see the Astra Linux Help Center website for instructions on how to enable/disable this mode (**Configuring protection and blocking mechanisms** in the **Blocking ptrace** section).

SUSE Linux Enterprise Server 15

Before installing the application on a device running the SUSE Linux Enterprise Server 15 operating system, the insserv-compat package must be installed.

ALT SP in closed software environment mode

Before installing the application on a device with the ALT SP operating system in closed software environment mode:

1. Disable the closed software environment mode:

   ```
   integrity-remover
   ```

2. Create a kesl group for further changes to the IMA policy:

   ```
   groupadd kesl
   ```

3. Find out the unique identifier (GID) of the created group:

   ```
   cat /etc/group | grep kesl
   ```

4. Edit the IMA policy to exclude the kesl group from the application components integrity check using the utility to make sure the application works correctly. To do so:

   a. Copy the /usr/share/integrity/policy file:

   ```
   cp /usr/share/integrity/policy /etc/integrity/policy
   ```

b. Open the /etc/integrity/policy file for editing in a text editor (for example, vim):

```
vim /etc/integrity/policy
```

c. After the `dont_measure fsmagic=0xf97cff8c` line (usually, this is the last line of the `dont_measure` section), add the line:

```
dont_measure fgroup=<GID>
```

where `<GID>` is an unique ID of the group created at step 2 of these instructions.

d. After the `dont_appraise fsmagic=0x27e0eb` line (usually, this is the last line of the `dont_appraise` section), add the line:

```
dont_appraise fgroup=<GID>
```

where `<GID>` is an unique ID of the group created at step 2 of these instructions.

e. Save your changes.

5. In the /usr/sbin/integrity-sign file, edit the list_all_files function to include the Kaspersky Endpoint Security application in the allowlist of applications that are allowed to run in the closed environment mode. To do so:

a. Open the /usr/sbin/integrity-sign file for editing in a text editor (for example, vim):

```
vim /usr/sbin/integrity-sign
```

b. Find the list_all_files function and in the body of the function, in lines starting with `find -P`, add the directories of the Kaspersky Endpoint Security application under /var/opt and /opt to the end of each enumeration of directories.

c. Save your changes.

During the initial configuration of the application, do not initiate the application database update.

After the installation is complete, enable the closed software environment mode and perform the actions required to start the application.

OSnova

If you intend to use Kaspersky Security Center to install and manage the application, prepare the device for the installation of Network Agent before installing the application:

1. Open the /usr/lib/systemd/logind.conf.d/10-enable-kill-user-processes.conf file for editing and in the `[Login]` section, comment out the KillUserProcesses=yes line.

```
#KillUserProcesses=yes
```

2. Open the /usr/lib/NESS/pam-user-session file for editing and comment out the loginctl terminate-session "$XDG_SESSION_ID" line.

```
#loginctl terminate-session "$XDG_SESSION_ID"
```

Operating systems with SELinux support

If the semanage utility is not installed in your operating system, before installing the application, install the policycoreutils-python or policycoreutils-python-utils package, depending on your package manager.

The policycoreutils-python-utils package is provided for the following types of package managers: dnf, apt, and yum for Fedora, Debian, Ubuntu, and RHEL 7 and newer.

The policycoreutils-python package is provided for the following types of package managers: yum and CentOS/RHEL 7 and older.

Kylin OS

Before installing the application on a Kylin OS device:

1. In the UKUI (Ubuntu Kylin User Interface), turn off Firewall. To do this, go to the **Kylin Security Center** → **Firewall and Network Protection** section and under **Firewall**, disable the **Public Network** and **Private network** toggle switches.

2. In the UKUI, disable Application Network Control. To do this, go to the **Kylin Security Center** → **Firewall and Network Protection** section and under **Application Network Control**, select **Disable**.

3. In the UKUI, disable Application Source Check. To do this, go to the **Kylin Security Center** → **Application Protection** section and under **Application Source Check**, select **Disable**.

4. Disable the KYSEC security mechanism. To do so, perform the following actions in the terminal:

   a. Check the current status:

   ```
   getstatus
   ```

   b. Disable the KYSEC security mechanism:

   ```
   setstatus disable -p
   ```

   c. Verify that the KYSEC security mechanism is disabled:

   ```
   getstatus
   ```

5. Uninstall the built-in anti-virus application. To do so, run the following command in the terminal:

```
sudo dpkg -P pksav
```

6. If you have the Qaxsafe anti-virus installed on your device, you need to uninstall it. To do so:

   a. Disable Self-Protection:

      1. Find the application icon in the notification area of the taskbar and double-click the application icon to open the context menu.

      2. In the context menu, select **Settings** → **Protection Center**.

      3. This opens a window; in that window, clear the **Enable Self-Protection** check box and enter a password if prompted.

   b. Uninstall the Qaxsafe antivirus. To do so, run the following command in the terminal:

```
sudo dpkg -P qaxsafe
```

   c. Delete any files left behind. To do so, run the following command in the terminal:

```
sudo rm -rf /opt/qaxsafe
```

Operating systems that do not support fanotify

Before proceeding with the installation of the application, make sure that the following is installed on the device:

- Packages for compiling applications and running tasks (gcc, binutils, glibc, glibc-devel, make)
- Package with header files of the operating system kernel for compiling Kaspersky Endpoint Security modules

Useful articles

Troubleshooting issues on Kylin OS

After preparing the environment for installation, you can go back to the deployment scenario and continue from the Selecting the system event interception mechanism step.

Selecting the system event interception mechanism

To function properly, the application must intercept system events for file operations and the starting of processes. System event interception is required in all application modes (Standard mode, Light Agent mode, and EDR agent mode). If the application does not use system event interception, real-time file scanning is not performed, and the protection level of the device is reduced.

System event interception mechanism

The application can use the following mechanisms to intercept system events:

- **System interception mechanism based on fanotify.** *Fanotify* is a subsystem of the Linux kernel that monitors events in the file system (for example, opening, reading, writing, or closing files) and allows applications to intercept these in real time.

- **Interception mechanism based on an updatable kernel module.** The *updatable kernel module* works in conjunction with the system interception mechanism based on the fanotify technology. This allows you to optimize the interception of file operations and the interception of process starts by Kaspersky Endpoint Security by processing system events in kernel space, and not in user space. The updatable kernel module intercepts file operations when files are opened, renamed, or modified. Application performance is increased thanks to the file and process scan results cache.

  The updatable kernel module is also used for the following tasks and components:

  - File Threat Protection
  - Anti-Cryptor
  - Exploit Prevention
  - Behavior Detection
  - Application Control
  - Execution Prevention for objects (when integrating with Kaspersky Endpoint Detection and Response Expert (on-premises) and Kaspersky Endpoint Detection and Response Optimum)

  By using the updatable kernel module, you can configure global exclusions in a more granular way. The interception mechanism based on the fanotify technology allows wholly excluding the specified mount points file operation interception. Using the updatable kernel module allows you to exclude specific local or remote directories mounted on the device.

  The updatable kernel module is included in the distribution kit of the application.

- **Kernel module for File Threat Protection on an operating system without fanotify**. If the operating system on the device does not support the fanotify technology (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), the application compiles and uses a special module to intercept system events. This module is automatically compiled when File Threat Protection is started, provided that all the dependencies and build tools are available.

How to choose a system event interception mechanism

If the operating system supports fanotify, you can select a system event interception mechanism when deploying the application: just fanotify or updatable kernel module plus fanotify. The default setting is fanotify. After installation, you can change the system event interception mechanism in application settings.

For operating systems that do not support fanotify, selection of interception mechanism is not available.

The application can use the interception mechanism based on the updatable kernel module if the operating system satisfies the requirements for installing the updatable kernel module.

Updatable kernel module installation requirements

To install and use the updatable kernel module, the device must have one of the following 64-bit operating systems installed:

- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6.5, 1.6.6).
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7.3, 1.7.4, 1.7.6, 1.7.7, 1.7.8, 1.7.9).
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.8.2, 1.8.3, 1.8.4, 1.8.5).

  If the Kaspersky Endpoint Security application is used in Basic mode, the updatable kernel module can be used on devices with Astra Linux operating systems in the closed software environment mode.

- CentOS 7.x.
- CentOS 8.x.
- Debian GNU/Linux 12.7, 12.8, 12.9, 12.10, 12.11, 12.12.
- Red Hat Enterprise Linux 7.4.
- Red Hat Enterprise Linux 8.10.
- SberLinux 8.10.
- SberLinux 9.0.1.
- SberLinux 9.1.
- SberLinux 9.6.
- SberLinux 9.7.
- SberOS 3.4.
- SberOS 3.5.
- Ubuntu 16.04 LTS.
- Ubuntu 18.04 LTS.
- Ubuntu 20.04 LTS.
- Ubuntu 22.04 LTS.
- Ubuntu 24.04 LTS.
- ALT SP Workstation release 10.
- ALT SP Server release 10.
- ALT Education 10.

- ALT Workstation 11.
- ALT Server 11.
- ALT Education 11.
- RED OS 7.3.
- RED OS 8.0.
- ROSA "Cobalt" 7.9 Workstation.
- ROSA "Cobalt" 7.9 Server.
- ROSA "Chrome" 12 Workstation.
- ROSA "Chrome" 12 Server.

32-bit operating systems, operating systems for the Arm architecture, and operating systems for the Elbrus architecture are not supported.

The updatable kernel module may conflict with some versions of the Linux kernel and some third-party applications.

Checking if the updatable kernel module can be installed

The version of the updatable kernel module does not depend on the version of Kaspersky Endpoint Security. The functionality of the updated kernel module is regularly expanded as part of Kaspersky Endpoint Security database and application module updates. Therefore, the list of supported operating systems above may not be exhaustive. To verify that your device satisfies the requirements for installing the updatable kernel module, use the Kaspersky ULKM tool.

How to check remotely using the Web Console or the Administration Console

1. Download the ulkmtool.zip archive from the application download page in the **Kaspersky Endpoint Security for Linux** section.
2. Create an installation package for the utility.

   How to create an installation package in the Web Console

   1. Place the downloaded ulkmtool.zip archive in a folder accessible to the Kaspersky Security Center Administration Server.
   2. In the main Web Console window, select one of the following sections:
      - **Device discovery and deployment** → **Deployment and assignment** → **Installation packages**.
      - **Operations** → **Repositories** → **Installation packages**.

A list of installation packages available on the Administration Server opens.

3. Click the **Add** button.

   The wizard for creating an installation package will start.

4. Select **Create an installation package from a file** as the installation package creation method.

5. Enter the name of the new installation package, click the **Browse** button and specify the path to the ulkmtool.zip archive that you downloaded.

6. Finish the wizard.

The installation package will be created and added to the list of installation packages.

How to create an installation package in the Administration Console

1. Unpack the ulkmtool.zip archive to a folder accessible to the Kaspersky Security Center Administration Server.

2. In the console tree, select **Additional** → **Remote installation** → **Installation packages**.

   A list of installation packages available on the Administration Server opens.

3. Click the **Create installation package** button.

   The wizard for creating an installation package will start.

4. Click the **Create an installation package for a Kaspersky application** button.

5. Enter the name of the new installation package and proceed to the next step of the wizard.

6. Click the **Browse** button and specify the path to the ulkmtool.kud file. The file is located in the folder where you unpacked the ulkmtool.zip archive.

   Proceed to the next step of the wizard.

7. Wait until the file is downloaded and finish the wizard.

The installation package will be created and added to the list of installation packages.

3. Install Kaspersky Security Center Network Agent on devices for which you want to check if they satisfy the requirements of the updatable kernel module. See Kaspersky Security Center Help for more details.

4. In the Kaspersky Security Center Web Console or Administration Console, create and run a remote installation task on the devices for which you want to check if they satisfy the requirements of the updatable kernel module. In the task settings, select the installation package you created.

   The task results for each device indicate whether the device supports the installation and operation of the updatable kernel module.

Based on task results of the task, each device gets a tag:

- *UpdatableKernelModule=No* means the device does not support updatable kernel module installation.

- *UpdatableKernelModule=Yes* means the device satisfies the requirements for installing and running the updatable kernel module.

You can use these tags to create device selections. For example, you can select devices that satisfy the updatable kernel module requirements and install Kaspersky Endpoint Security with the updatable kernel module on these devices.

How to check locally on the device

1. Download the ulkmtool.zip archive from the application download page in the **Kaspersky Endpoint Security for Linux** section.

2. Install Kaspersky Security Center Network Agent on devices for which you want to check if they satisfy the requirements of the updatable kernel module. See Kaspersky Security Center Help for more details.

3. Run the Kaspersky ULKM tool utility locally on the devices that you want to scan.

   ```
   ulkmtool --check remote
   ```

4. Check return code.

   ```
   echo $?
   ```

   The utility returns the following codes on the command line:

   0 = Success means the device satisfies the requirements for installing and running the updatable kernel module.

   1 = NotSupported means the device does not support updatable kernel module installation.

Checking the status of the updatable kernel module

In Kaspersky Security Center Web Console or in the Administration Console, you can check the status of the updatable kernel module on devices with Kaspersky Endpoint Security. To do this, you can view the tags assigned to devices:

- *UpdatableKernelModule=Use* means the updatable kernel module is installed and running on the device.

- *UpdatableKernelModule=Error* means the updatable kernel module is installed on the device, but an error occurred when starting the module, and the module is not running.

For more details about viewing tags assigned to devices, refer to the Kaspersky Security Center Help.

Secure Boot support

The updatable kernel module supports Secure Boot. To use the interception mechanism based on the updatable kernel module on operating systems with Secure Boot enabled, you need to add the public certificate of Kaspersky Endpoint Security that the module is signed with to the operating system and then restart the operating system.

Download the certificate

Example of adding a certificate for Ubuntu

1. Make sure Secure Boot is enabled in your operating system:

```
mokutil --sb-state
```

2. Add the downloaded certificate to your operating system using the mokutil utility:

```
mokutil --import <path to certificate>
```

3. Restart Kaspersky Endpoint Security.

4. Check if the updatable kernel module is working by running the following command:

```
kesl-control --app-info
```

After selecting the system event interception mechanism, you can go back to the deployment scenario and continue from the Preparing distribution packages step.

Preparing distribution packages

The *Kaspersky Endpoint Security distribution package* is a set of files for installing and updating the application, as well as the texts of the user agreements (End User License Agreement, Privacy Policy, and Kaspersky Security Network Statement). You can also separately download the distribution package that includes a graphical interface for the convenience of locally managing and monitoring of the application.

You will need distribution packages to create an installation package for deployment on devices in the corporate network using Kaspersky Security Center, as well as for deploying the application using the command line.

For deployment using Kaspersky Security Center, you will also need a *distribution package for remote installation of the application*. This distribution package contains the files necessary for remote deployment of the application and the texts of user agreements.

> Texts of user agreements are available at the Kaspersky website (in the **EULA** section), as well as in the `/opt/kaspersky/kesl/doc/` directory after installing the application.

You can select the distribution packages for deploying Kaspersky Endpoint Security on your own or using Kaspersky Security Center at the Creating an installation package step.

How to choose a distribution package for Kaspersky Endpoint Security deployment

The choice of distribution packages depends on the following factors:

- Kaspersky Endpoint Security version: certified or not certified
- Deployment method: using Kaspersky Security Center or using the command line

- Package format depending on the OS
- Operating system architecture and CPU type
- Kaspersky Endpoint Security management method
- Necessity of installing the graphical user interface of the application

1. **Determine your version of the application, certified or not certified**

   - If you need the **certified** version, download the set of distribution packages from the Business applications support lifecycle page.

     The certified version contains the main application files and the graphical interface files (the `kesl` directory), an archive for remote application installation (the `remote install` directory), the MMC plug-in (`SCPlugin`) and the web plug-in (`web plugin`).

     Go to step 3.

   - If you need the **uncertified** version, go to the next step.

2. **Determine the deployment method: using Kaspersky Security Center or using the command line**

   For **deployment using Kaspersky Security Center**, download the distribution package from one of the sources:

   - From the Kaspersky website
   - By making a request to Technical Support if you have a Kaspersky CompanyAccount

   For **deployment using the command line**, download the distribution package from the Kaspersky website:

   - The main application distribution package (`Distributive`)
   - If necessary, the distribution package with the graphical user interface (`Product GUI`)

   If you want to download the distribution packages from the Kaspersky website, you will need the following files:

   - The main application distribution package (`Distributive`)
   - If necessary, the distribution package with the graphical user interface (`Product GUI`)
   - Distribution package for remote installation of the application using Kaspersky Security Center (**Additional distributive** → `Files for Product remote installation`)
   - Distribution package of Kaspersky Security Center Network Agent (Kaspersky Security Center distribution section → `Network agent`)

   The distribution package of the application is the same for all localizations. The language of Kaspersky Endpoint Security is selected during the initial configuration of the application. Localization support depends on the languages that are installed in the operating system.

3. **Determine the package format depending on the operating system of the protected device**

Operating system	Package format
Debian, Ubuntu, Astra Linux, Linux Mint	`.deb`
Red Hat Enterprise Linux, CentOS, Oracle Linux, RED OS, SUSE Linux Enterprise, openSUSE, Rocky Linux, AlmaLinux, OS from the ALT series, GosLinux, OS from the Rosa series, Amazon Linux 2023	`.rpm`

If your operating system is not listed, select the package format in accordance with the documentation of your operating system.

4 **Determine the architecture of the operating system and CPU type**

CPU type and bitness of the operating system	Distribution package
Arm CPU, 64-bit operating system	`arm64` `aarch64`
Elbrus CPU	`e2k`
Other processors, 32-bit operating system	`i386`

Other processors, 64-bit operating system	`x86_64`
	`x64`
	`amd64`

To install the Kaspersky Endpoint Security application on operating systems with limited support (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), select the distribution package marked `OLD`.

Editing configuration files of the application on your on using means not described in the application documentation or not recommended by Technical Support may cause poor performance and failures of the application and operating system, reduced protection of your device, inaccessible and corrupted data, as well as the sending of additional statistics to KSN getting turned on.

After preparing the distribution packages, you can go back to the deployment scenario and continue from the Preparatory actions in Kaspersky Security Center step.

Preparatory actions in Kaspersky Security Center

Before installing the Kaspersky Endpoint Security application, we recommend doing the following in Kaspersky Security Center.

1 Configuring administration groups for devices

To manage the application using Kaspersky Security Center, you need to place devices on which the application is installed in administration groups. By default, Kaspersky Security Center moves all the devices that have the Administration Agent installed and are connected to Administration Server to the **Unassigned devices** group.

We recommend configuring rules for automatic placement of devices in administration groups in advance and allocating devices to groups in accordance with their type by creating a separate group for each type of device. This lets you apply different application settings depending on your device.

You can also place devices in administration groups manually.

2 Installation and initial configuration of the Network Agent

Network Agent facilitates the device connection to the Kaspersky Security Center Administration Server. It must be installed on every device that will be connected to Kaspersky Security Center.

1. Prepare your Linux devices for Network Agent installation. The procedure depends on the operating system.

2. Perform the installation and initial configuration of Network Agent. See Kaspersky Security Center Help for instructions.

As a result, devices with Network Agent installed are displayed in the group corresponding to the moving rules configured for these devices. If you have not configured any moving rules, the devices are displayed in the **Unassigned devices** group.

3 Installing the Kaspersky Endpoint Security management plug-in

Install a Kaspersky Endpoint Security management plug-in depending on the Kaspersky Security Center management console that you are using:

- The **Kaspersky Endpoint Security administration MMC plug-in** lets you manage the application using Kaspersky Security Center Administration Console. The MMC plug-in is installed on the device where Kaspersky Security Center Administration Console is installed.

  How to install the Kaspersky Endpoint Security MMC plug-in

  > Before installing Kaspersky Endpoint Security MMC management plug-in, make sure that Kaspersky Security Center and Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable) are installed.

  To install the MMC plug-in:

  1. Download the klcfginst.msi file on the application download page in the **Kaspersky Endpoint Security for Linux** section (**Build** → **Administration Plug-In**).

  2. On the device where the Kaspersky Security Center Administration Console is installed, run the klcfginst.msi file.

  After installation, the MMC management plug-in is displayed in the list of installed MMC management plug-ins in the properties of the Kaspersky Security Center Administration Server.

To view the list of installed management MMC plug-ins:

1. In the Kaspersky Security Center Administration Console tree, select the **Administration Server <server name>** node and open the Administration Server properties window in one of the following ways:

   - Open the context menu of the **Administration Server <server name>** node and select the **Properties** item.

   - Click the **Administration Server properties** link in the workspace of the **Administration Server <server name>** node in the **Administration Server** section.

2. In the list on the left, in the **Advanced** section, select the **Information about the installed application management plug-ins** section.

   In the right part of the window, the list of installed administration plug-ins displays the administration MMC plug-in for Kaspersky Endpoint Security: **Kaspersky Endpoint Security <version number> for Linux**.

If you use the Kaspersky Security Center Administration Console to manage the Kaspersky Endpoint Security application and you have multiple versions of the application installed, you need to install a management plug-in each version of the Kaspersky Endpoint Security application. This allows you to manage the application by using the policies created with different administration plug-in versions. You can also convert policies and tasks created with previous versions of the administration plug-in to newer versions.

- The **Kaspersky Endpoint Security management web plug-in** lets you manage the application using Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console. The web plug-in is installed on the device that has the Kaspersky Security Center Web Console installed. The functionality of the web plug-in is available to all administrators who have access to Kaspersky Security Center Web Console in a browser.

  How to install the Kaspersky Endpoint Security web plug-in

  You can install the web plug-in:

  - Using the Quick Start Wizard for Kaspersky Security Center Web Console.

    Kaspersky Security Center Web Console automatically prompts you to run the Quick Start Wizard when connecting Kaspersky Security Center Web Console to the Administration Server for the first time. You can also run the Initial Configuration Wizard in the Kaspersky Security Center Web Console interface (**Device discovery and deployment** → **Deployment and assignment** → **Quick Start Wizard**). The Quick Start Wizard can also check if the installed web plug-ins are up to date and download the necessary updates. For details on the Quick Start Wizard for Kaspersky Security Center Web Console, refer to the Kaspersky Security Center Help.

  - Manually, using a distribution kit from the list of Kaspersky Web plug-ins or from a file.

  To install the Kaspersky Endpoint Security web plug-in manually from Kaspersky Security Center:

  1. In the main window of the Kaspersky Security Center Web Console, select **Settings** → **Web plug-ins**.

     A list of installed web plug-ins opens.

  2. Click the **Add** button.

     This opens the list of available management plug-ins. The list is updated automatically after new versions of web plug-ins are released.

  3. In the list of available plug-ins, select the **Kaspersky Endpoint Security <version number> for Linux** web plug-in.

4. In the window that opens with a description of the web plug-in, click the **Install plug-in** button.

5. Wait for the installation to complete and click **OK** in the information window.

The new plug-in will be displayed in the list of installed web plug-ins (**Settings** → **Web plug-ins**).

To install the Kaspersky Endpoint Security web plug-in manually from a file:

1. Download the archive with the Web Plug-in from the application download page in the **Kaspersky Endpoint Security for Linux** section (**Additional distribution package** → **Web console Plug-in**).

2. Unpack the downloaded archive locally.

3. In the main window of the Kaspersky Security Center Web Console, select **Settings** → **Web plug-ins**.

   A list of installed web plug-ins opens.

4. Click the **Add from file** button.

5. This opens a window; in that window, specify the path to the plugin.zip file and the path to the signature.txt file. The files are located in the folder to which you unpacked the archive with the Web Plug-in.

6. Click the **Add** button.

7. Wait for the installation to complete and click **OK** in the information window.

The new plug-in is displayed in the list of installed web plug-ins (**Settings** → **Web Plug-ins**).

If you select a language that is not included in Kaspersky Endpoint Security distribution package in the properties of Kaspersky Security Center Administration Server, the License Agreement and the entire Kaspersky Security Center Web Console interface will be displayed in English.

Video: Installing the management web plug-in using the wizard

Video: Installing the management web plug-in in isolated networks

4 Creating a Kaspersky Endpoint Security policy

Create a policy for Kaspersky Endpoint Security in Kaspersky Security Center Web Console or in the Administration Console (depending on the Kaspersky Security Center management console that you are using).

Manage the following settings depending on the mode in which you want to use the application:

For Standard mode

If you have created a policy in the Administration Console wizard, specify the application usage mode: **Standard mode or Endpoint Detection and Response Agent Mode**. If you have created a policy in the Kaspersky Security Center Web Console wizard, skip the selection of application mode.

For EDR agent mode

1. If you have created a policy in the Administration Console wizard, specify the application usage mode: **Standard mode or Endpoint Detection and Response Agent Mode**. If you have created a policy in the Kaspersky Security Center Web Console wizard, skip the selection of application mode.

2. Complete the policy creation by following the instructions of the wizard.

3. Open the properties of the created policy in the Kaspersky Security Center Web Console or the Administration Console and enable integration with the Detection and Response solutions that you want to use to protect the device:

   - For Kaspersky Endpoint Detection and Response Expert (on-premises) Integration on the OSMP platform, you need to enable and configure the EDR Expert (on-premises) component. The settings are available in the Kaspersky Security Center Web Console

   - For integration with Kaspersky Endpoint Detection and Response on the Kaspersky Anti Targeted Attack Platform, you need to enable and configure the EDR Expert (on-premises) component. The settings are available in the Kaspersky Security Center Web Console and the Administration Console.

   - For integration with Kaspersky Network Detection and Response on the Kaspersky Anti Targeted Attack Platform, you need to enable and configure the NDR (KATA) component. The settings are available in the Kaspersky Security Center Web Console and the Administration Console.

For Light Agent mode

In the New policy wizard:

1. Specify the **Light Agent mode for protecting virtual environments**.

2. Manage SVM discovery settings:

   a. Select the method that Light Agents use to discover SVMs available for connection.

      - **Use Integration Server**. If this option is selected, Light Agent connects to Integration Server to get a list of SVMs available for connection and their details.

      - **Use a custom list of SVM addresses**. If this option is selected, you can specify a list of SVMs that Light Agents managed by this policy can connect to. Light agents will only connect to SVMs specified in the list.

      If you select the **Use a custom list of SVM addresses** option, the Light Agent is using the extended SVM selection algorithm, and large infrastructure protection mode is enabled on an SVM, then connecting a Light Agent to this SVM is only possible if the SVM path is ignored. In the **SVM selection algorithm** section, you need to set the **SVM path** setting to **Ignore**. If any other value is set, Light Agents will not be able to connect to the SVM. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

   b. If you select Integration Server, the wizard displays the current settings for connecting Light Agents to the Integration Server: address and port for connecting. If necessary, specify new connection settings: IPv4 address or fully qualified domain name (FQDN) and port for connecting to the Integration Server.

      If a Linux-based high-availability cluster of Integration Servers is deployed in your infrastructure, you need to specify the address and port of the load balancer as the address and port for connecting to the Integration Server. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

   c. If you select a manually defined list of SVM addresses, create a list of SVMs that Light Agents managed by this policy can connect to. To add an SVM to the list, click the **Add** button and, in the window that opens, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line.

      Specify only fully qualified domain names (FQDNs) that map to a single IP address. Using a fully qualified domain name that corresponds to multiple IP addresses can lead to errors in the application.

For the rest of the policy settings, you can leave the default values. The default settings provide a basic level of protection. After installing Kaspersky Endpoint Security, you can configure the policy in accordance with the requirements of your organization. To do this, you can use the component configuration scenarios from the Managing the application Help section.

Video: creating a policy

5 Configuring centralized updates of application databases and modules

By default, Kaspersky Endpoint Security is installed on a device without anti-virus databases. The application becomes functional only after the databases are downloaded to the device. To make sure the protection begins immediately after the application is installed, configure centralized database updates.

In Kaspersky Security Center Web Console or in the Administration Console (depending on the Kaspersky Security Center management console that you are using):

1. Start the Administration Server task *Download updates to the Administration Server repository*. The task is created automatically by the Administration Server Quick Start Wizard.

   The task downloads the update package for Kaspersky Endpoint Security to the updates directory on the Administration Server.

2. Create a group task of the *Update* type for the Kaspersky Endpoint Security application. In task settings, specify:

   - Update source: Kaspersky Security Center.
   - Task schedule: at least daily. We recommend running the task 4 to 6 times a day.

Video: configuring centralized database updates

6 Adding license keys and creating an activation task

To activate the application in standard mode, you must add a license key to the application. If some components are not covered by your license, you may need another license key:

To activate the Kaspersky Endpoint Security application in EDR agent mode, you need an EDR Expert (on-premises) license key.

You can choose an activation method depending on your infrastructure and the requirements of your organization:

- If the application is installed on all your devices with the same set of functionality, use automatic distribution of license keys. The license key to be distributed must first be added to the Kaspersky Security Center key store using a key file or activation code. For more information, see the Kaspersky Security Center Help.

- If the sets of application functionality differ from device to device, you will need different license keys for activation. In this case, place the protected devices in different administration groups and configure a group task for adding a key for each administration group.

Kaspersky Endpoint Security in Light Agent mode receives license information from the Protection Server after connecting to the SVM. You do not need to separately activate Kaspersky Endpoint Security in Light Agent mode.

Video: Activating the application with an activation code

Video: Activating the application with a key file

Having prepared Kaspersky Security Center, you can go back to the deployment scenario and continue from the Installing the application step.

Installing the application using Kaspersky Security Center

Special considerations involved in installation:

- EDR Agent mode and Light Agent mode of Kaspersky Endpoint Security are not supported on devices with an Elbrus CPU.
- On Arm devices, Kaspersky Endpoint Security in Light Agent mode is not supported.

The recommended scenario for installing the application using Kaspersky Security Center involves the following steps:

You can also install the Kaspersky Endpoint Security application via Kaspersky Security Center using the Quick start wizard and the Protection deployment wizard.

1 Creating an installation package

The installation package of the Kaspersky Endpoint Security application contains the following:

- The main distribution package
- A distribution package for remote installation of the application
- A distribution package with the graphical interface of the application
- Initial configuration settings that are applied during installation

You can create an installation package in the following ways:

- **Using a distribution package hosted on Kaspersky servers**. In Kaspersky Security Center, an installation package is automatically created from the specified distribution package.

  Video: automatic creation of an installation package in Kaspersky Security Center

  To install the Kaspersky Endpoint Security application on operating systems with limited support (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6), select the distribution package marked `for legacy OS`.

- **Manually, using files prepared at the Preparing distribution packages step**. This method is recommended if you want to specify the initial configuration settings using a configuration file or if you want to use the created installation package for different operating systems or different package managers.

Video: manually creating an installation package in Kaspersky Security Center

You can add pre-downloaded application databases to the installation package. If you are using an installation package with integrated databases, the application is installed together with the databases; in this case, you do not need to update the databases immediately after installation.

You can use the same installation package many times.

How to prepare an installation package manually

1. Locally unpack the archive with files for remote installation of Kaspersky Endpoint Security.

2. Place the packages with the main application files in the same directory.

   If you want to use the created installation package with different operating systems or package managers, place the distribution packages for all the types of operating systems and package managers that you need in the directory.

3. If you want to use the graphical interface of the application, place the graphical interface packages in the same directory.

   Enable the use of the graphical interface by editing the appropriate setting (`USE_GUI=Yes`) in the properties of the created installation package or in the autoinstall.ini configuration file. By default, the graphical interface is not installed.

   > If Kaspersky Endpoint Security is used in Light Agent mode, the graphical user interface is not supported.

4. If you want to set up the initial configuration of the application using a configuration file, open the autoinstall.ini configuration file and edit it as necessary. The autoinstall.ini file is located in the folder to which you unpacked the archive with the files for remote installation of Kaspersky Endpoint Security.

   a. The application is used in standard mode by default.

      To use the application in EDR Agent mode, set `ENDPOINT_AGENT_MODE=Yes`.

      To use the application in Light Agent mode, set `KSVLA_MODE=Yes`.

      > After Kaspersky Endpoint Security is installed, you cannot change the application usage mode.

b. To install the application in Light Agent mode:

- If you are installing the application on a template from which temporary virtual machines will be created, set `VDI_MODE=Yes`. This setting enables VDI protection mode to optimize application performance on temporary virtual machines.

- Specify the role in the virtual infrastructure (server or workstation) of the virtual machines that you want to protect (`SERVER_MODE=Yes|No`). The role of a virtual machine determines the license under which the application will be used on this virtual machine as well as the available functionality.

You can also change the initial configuration of the application later in the properties of the created installation package on the **Settings** tab.

5. Place all prepared files in an archive in ZIP, CAB, TAR, or TAR.GZ format with any name.

How to create an installation package in the Web Console

1. In the main Web Console window, select one of the following sections:

   - **Discovery & deployment** → **Deployment & assignment** → **Installation packages**.

   - **Operations** → **Repositories** → **Installation packages**.

   A list of installation packages available on the Administration Server opens.

2. Click the **Add** button.

   The wizard for creating an installation package will start.

3. If you are using the Web Console, select how you want to create an installation package:

   - **Create an installation package from a file**. The installation package will be created from an archive that you have prepared in advance.

   - **Create an installation package for a Kaspersky application**. The installation package will be created from a distribution package located on Kaspersky servers.

   If you are using the Kaspersky Security Center Cloud Console, the installation package is created from the distribution package hosted on Kaspersky servers.

4. Depending on the package creation method:

   - Specify the package name, click the **Browse** button, and specify the path to the archive that you have prepared for creating the installation package.

   - Select Kaspersky Endpoint Security distribution package. In the window on the right, read the information about the distribution package and click the **Download and create installation package** button. The installation package creation process starts.

5. Read the End User License Agreement concluded between you and Kaspersky, and the Privacy Policy describing the handling and transmission of data. To continue creating the installation package, you must confirm that you have read and accept the full terms of the End User License Agreement and the Privacy Policy.

6. Finish the wizard.

   The installation package will be created and added to the list of installation packages.

7. Open the properties of the installation package and go to the **Settings** tab.

   - If you are installing the application in EDR Agent mode, for the **Usage mode** setting, select **Endpoint Detection and Response Agent**.

   - If you are installing the application in Light Agent mode, specify the following settings:

     Usage mode, select the **Light Agent to protect virtual environments** option.

     Enable VDI protection mode. Select this check box to enable VDI protection mode. This is recommended if you are installing the application on a virtual machine template that will be used to create temporary virtual machines. This check box is cleared by default.

     The protected virtual machine is used as a server. The role of the virtual machine on which the application will be installed: server or workstation. By default, this check box is selected (the virtual machine is used in the virtual infrastructure as a server).

   - If necessary, manage other initial configuration settings.

     For a description of all the initial configuration settings of the application in the installation package, see Appendix 1.

How to create an installation package in the Administration Console

To create an installation package using prepared files:

1. In the console tree, select **Additional** → **Remote installation** → **Installation packages**.

2. Click the **Create installation package** button.

   The wizard for creating an installation package will start.

3. Click the **Create an installation package for a Kaspersky application** button.

4. Enter the name of the new installation package and proceed to the next step of the wizard.

5. Specify the path to the kesl.kud file. The file is located in the folder to which you unpacked the archive with the files for installing the application (kesl.zip) at the Preparing distribution packages step.

   The name and version of the application are displayed in the window. Proceed to the next step of the wizard.

6. Read the End User License Agreement concluded between you and Kaspersky, and the Privacy Policy describing the handling and transmission of data.

   To continue, confirm that you have read and accept the full terms of the End User License Agreement and the Privacy Policy. To confirm, in the window that opens, select both check boxes.

   Proceed to the next step of the wizard.

7. The wizard downloads the files required to install the application to Kaspersky Security Center Administration Server. Wait until the download is complete and finish the wizard.

8. Open the properties of the installation package and go to the **Application settings** tab.

   - If you are installing the application in EDR Agent mode, for the **Application mode** setting, select **Endpoint Detection and Response Agent**.

   - If you are installing the application in Light Agent mode, specify the following settings:

     Application mode. Select the **Light Agent for protecting virtual environments** option.

Enable VDI protection mode. Select this check box to enable VDI protection mode. This is recommended if you are installing the application on a virtual machine template that will be used to create temporary virtual machines. This check box is cleared by default.

The protected virtual machine is used as a server. The role of the virtual machine on which the application will be installed: server or workstation. This check box is selected by default.

Unavailable in Light Agent mode:

- Configuring update sources for the application databases and starting an update
- Configuring proxy server settings
- Application activation

The application in Light Agent mode receives database updates and license information from the Protection Server after connecting to the SVM. You do not need to separately activate Kaspersky Endpoint Security or configure database updates.

- If necessary, manage other initial configuration settings.

  For a description of all the initial configuration settings of the application in the installation package, see Appendix 1.

You can perform the initial configuration of the application later in the properties of the created installation package in the **Application settings** section.

The wizard creates an installation package based on the distribution package from Kaspersky servers.

1. In the console tree, select **Additional** → **Remote installation** → **Installation packages**.
2. Click the **Additional actions** → **View current versions of Kaspersky applications** button.
3. Select the Kaspersky Endpoint Security distribution package from the list and click the **Download and create installation package** button.
4. Read the End User License Agreement concluded between you and Kaspersky, and the Privacy Policy describing the handling and transmission of data.

   To continue, confirm that you have read and accept the full terms of the End User License Agreement and the Privacy Policy. To confirm, select both check boxes in the confirmation window and click the **Accept all** button.
5. Wait for the download to finish. The installation package will be created and added to the list of installation packages.
6. Open the properties of the installation package and go to the **Application settings** section.

   - If you are installing the application in EDR Agent mode, for the **Application mode** setting, select **Endpoint Detection and Response Agent**.
   - If you are installing the application in Light Agent mode, specify the following settings:

     Application mode. Select the **Light Agent for protecting virtual environments** option.

     Enable VDI protection mode. Select this check box to enable VDI protection mode. This is recommended if you are installing the application on a virtual machine template that will be used to create temporary virtual machines. This check box is cleared by default.

     The protected virtual machine is used as a server. The role of the virtual machine on which the application will be installed: server or workstation. This check box is selected by default.

The following settings are not available in Light Agent mode:

- Configuring update sources for the application databases and starting an update
- Configuring proxy server settings
- Application activation

The application in Light Agent mode receives database updates and license information from the Protection Server after connecting to the SVM. You do not need to separately activate Kaspersky Endpoint Security or configure database updates.

- If necessary, manage other initial configuration settings.

  For a description of all the initial configuration settings of the application in the installation package, see Appendix 1.

You can perform the initial configuration of the application later in the properties of the created installation package in the **Application settings** section.

2 Installing the application on devices in the corporate network

You can install the application via the Kaspersky Security Center using the remote application installation task.

If necessary, you can view the application remote installation log by using remote diagnostics of the Kaspersky Security Center client device.

The initial configuration of the application is performed automatically in accordance with the settings made in the properties installation package or in the configuration file included in the installation package.

Video: installing, updating databases and checking the performance of Kaspersky Endpoint Security

3 Application database update

If you have installed the application in standard mode or EDR Agent mode, Run the *Update* group task created at the "Configuring centralized updates of application databases and modules" step in the Web Console or in the Administration Console (depending on the Kaspersky Security Center management console that you are using). For more information about updating the databases of Kaspersky Endpoint Security, see the Updating application databases and modules section.

4 Application health check

As a result, the Kaspersky Endpoint Security application has been installed, activated, and the application databases have been updated. After installation, the application starts automatically. By default, the following components are enabled:

- File Threat Protection.
- Device Control.
- Behavior Detection.
- Web Threat Protection—only if one of the supported browsers is installed in the operating system and local management of Web Threat Protection settings is allowed on the device (a policy is not applied or the "lock" is not set in the policy properties).
- Network Threat Protection—only if the Network Threat Protection settings on the device are defined through a policy. Network Threat Protection is enabled in the policy properties by default. If locally configured settings are applied on the device, Network Threat Protection is disabled by default.

Verify that the application is ready for use.

How to check the protection status of a device in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.

   This opens the properties window for the managed device.

4. On the **General** tab, select the **Protection** section. The **Device status** field should display *OK*.

   If the **Device status** field displays information about insufficient rights to system directories, check the permissions for the following directories locally on this device: /var/opt/kaspersky, /var/log/kaspersky, and /opt/kaspersky. Make sure that the owner is root and that only the owner has write access to these directories.

5. Go to the **Applications** tab.

6. In the list of applications installed on the device, click Kaspersky Endpoint Security.

   The application properties window opens.

7. Look under **Application databases** on the **General** tab in the **Information** section. Make sure the application databases are up to date.

8. Go to the **Licenses** section on the **General** tab and make sure the application is activated.

9. If you have installed the application in EDR Agent mode, go to the **Components** section on the **General** tab and make sure that the integrations that you configured at the "Creating a Kaspersky Endpoint Security policy" step have the *Running* status.

10. If you have installed the application in Light Agent mode, go to the **Components** section on the **General** tab and make sure that the **Light Agent mode for protecting virtual environments** line displays the status as *running*. This means that the application is being used in Light Agent mode.

How to check the protection status of a device in the Administration Console

1. In the Administration Console tree, in the **Managed devices** folder, select the administration group containing the necessary device.

2. In the workspace, select the **Devices** tab.

3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.

   This opens the properties window for the managed device.

4. Select the **Protection** section. The **Device status** field should display *OK/Visible in the network*.

   If the **Device status** field displays information about insufficient rights to system directories, check the permissions for the following directories locally on this device: /var/opt/kaspersky, /var/log/kaspersky, and /opt/kaspersky. Make sure that the owner is root and that only the owner has write access to these directories.

5. Go to the **Applications** section.

6. In the list of applications installed on the device, select the Kaspersky Endpoint Security application and double-click to open the application properties window.

7. Look at the **Application databases** field in the **General** section. Make sure the application databases are up to date.

8. Go to the **License keys** section and confirm that the application is activated.

9. If you have installed the application in EDR Agent mode, go to the **Components** section and make sure that the integrations that you configured at the "Creating a Kaspersky Endpoint Security policy" step have the *Running* status.

10. If you have installed the application in Light Agent mode, go to the **Components** section and make sure that the **Light Agent mode for protecting virtual environments** line displays the *running* status. This means that the application is being used in Light Agent mode.

Useful articles

What to do if tasks do not run or policies are not applied

What to do if the device has the status: "Invalid policy settings. Policy has not been applied."

Error: "Application is not supported by the current version of Kaspersky Security Center Web Console or application web plug-in is not installed"

Troubleshooting an issue when installing the GUI

Description of installation error codes

Errors following Kaspersky Endpoint Security installation

After you have installed Kaspersky Endpoint Security, you can go back to the deployment scenario and continue from the Additional configuration steps after installation in certain operating systems step.

Installing the application using the command line

Special considerations involved in installation:

- EDR Agent mode and Light Agent mode of Kaspersky Endpoint Security are not supported on devices with an Elbrus CPU.
- On Arm devices, Kaspersky Endpoint Security in Light Agent mode is not supported.
- You need root privileges to install the application and graphical interface.
- You must run the Initial Configuration Wizard as root.
- If the version of the apt package manager is lower than 1.1.X, you need to use the dpkg package manager (depending on the operating system) for installation.

The recommended scenario for installing the application using the command line involves the following steps:

1 Installing the Kaspersky Endpoint Security application

Before starting the installation, place the downloaded package with the main files of the application in the /tmp directory on the device.

How to install the application from an RPM package

On a 32-bit operating system

```
yum install kesl-12.5.0-<build number>.i386.rpm
```

On a 64-bit operating system

```
yum install kesl-12.5.0-<build number>.x86_64.rpm
```

On a 64-bit ALT operating system

```
apt-get install kesl-12.5.0-<build number>.x86_64.rpm
```

On a 64-bit operating system for the Arm architecture

```
yum install kesl-12.5.0-<build number>.aarch64.rpm
```

On a 64-bit ALT operating system for the Arm architecture

```
apt-get install kesl-12.5.0-<build number>.aarch64.rpm
```

On a 64-bit operating system for the Elbrus architecture

```
yum install kesl-12.5.0-<build number>.2ek.rpm
```

On a 64-bit ALT operating system for the Elbrus architecture

```
apt-get install kesl-12.5.0-<build number>.2ek.rpm
```

On a 64-bit operating system with limited support (CentOS 5.2, CentOS 5.4, CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-12.5.0-<build number>.x86_64.rpm
```

To install the application on CentOS 5.2, CentOS 5.4, CentOS 6.4, or CentOS 6.6, you need to download the distribution package marked `OLD` from the website.

How to install the application from a DEB package

On a 32-bit operating system

```
apt-get install ./kesl_12.5.0-<build number>_i386.deb
```

On a 64-bit operating system

```
apt-get install ./kesl_12.5.0-<build number>_amd64.deb
```

On a 64-bit operating system for the Arm architecture

```
apt-get install ./kesl_12.5.0-<build number>_arm64.deb
```

On a 64-bit operating system for the Elbrus architecture

```
apt-get install ./kesl_12.5.0-<build number>_2ek.deb
```

2 Installing the graphical interface of the application

If you want to manage the application using the graphical interface, you need to install the graphical interface on the same device as the application.

Special features of the application graphical interface:

- You cannot install the graphical interface on a device where the Kaspersky Endpoint Security application is not installed.
- If the application is used in Light Agent mode, the graphical user interface is not supported.

Before starting the installation, place the downloaded package with the files of the application graphical interface in the /tmp directory on the device.

How to install the graphical interface of the application from an RPM package

On a 32-bit operating system

```
yum install kesl-gui-12.5.0-<build number>.i386.rpm
```

On a 64-bit operating system

```
yum install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

On a 64-bit ALT operating system

```
apt-get install kesl-gui-12.5.0-<build number>.x86_64.rpm
```

On a 64-bit operating system for the Arm architecture

```
yum install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

On a 64-bit ALT operating system for the Arm architecture

```
apt-get install kesl-gui-12.5.0-<build number>.aarch64.rpm
```

On a 64-bit operating system on the Elbrus architecture

```
yum install kesl-gui-12.5.0-<build number>.2ek.rpm
```

On a 64-bit ALT operating system on the Elbrus architecture

```
apt-get install kesl-gui-12.5.0-<build number>.2ek.rpm
```

On a 64-bit operating system with limited support (CentOS 6.4, CentOS 6.6)

```
rpm -i kesl-gui-12.5.0-<build number>.x86_64.rpm
```

To install the application on CentOS 6.4 or CentOS 6.6, you need to download the distribution package marked `OLD` from the website.

How to install the graphical interface of the application from a DEB package

```
On a 32-bit operating system
```

```
apt-get install ./kesl-gui_12.5.0-<build number>_i386.deb
```

```
On a 64-bit operating system
```

```
apt-get install ./kesl-gui_12.5.0-<build number>_amd64.deb
```

```
On a 64-bit operating system for the Arm architecture
```

```
apt-get install ./kesl-gui_12.5.0-<build number>_arm64.deb
```

```
On a 64-bit operating system for the Elbrus architecture
```

```
apt-get install ./kesl-gui_12.5.0-<build number>_2ek.deb
```

3 Initial setup of the application

The application needs initial configuration to prepare it for operation and enable the protection of the client device.

If initial configuration of the application has not been completed on a device, you cannot use or update the application on that device.

Initial configuration of the application is performed using the Initial Configuration Wizard from the distribution kit of Kaspersky Endpoint Security. You can perform the initial configuration in interactive mode or in automatic mode.

How to perform the initial configuration of the application interactively.

Step 1. Starting the wizard

```
Start the Initial Configuration Wizard
```

```
/opt/kaspersky/kesl/bin/kesl-setup.pl
```

At the prompt of the Wizard, specify the values of the initial configuration settings of Kaspersky Endpoint Security step by step.

If the Network Agent is installed on the device and you are installing the application in standard mode or EDR agent mode, you can skip the Initial Configuration Wizard steps related to updating the application databases and activating the application.

Step 2. Selecting the Standard mode or Light Agent mode

Enter `yes` to use the application in Light Agent mode.

Enter `no` to use the application in standard mode.

If you intend to use the application in EDR Agent mode, at this step, you need to enter `no` and select the EDR Agent mode at the next step.

After the initial configuration is complete, you cannot change the application usage mode.

Step 3. Selecting the mode: Standard or Endpoint Detection and Response Agent

The step is displayed if you chose to use the application in Standard mode at step 2.

Enter `yes` to use the application in EDR Agent mode.

Enter `no` to use the application in standard mode.

After the initial configuration is complete, you cannot change the application usage mode.

Step 4. Kaspersky Endpoint Detection and Response Expert (cloud) integration

The step is displayed if you chose to use the application in Standard mode at step 3.

Enter `yes` to use the Kaspersky Endpoint Detection and Response Expert (cloud) integration.

Enter `no` to use the Kaspersky Endpoint Detection and Response Expert (on-premises) integration.

Step 5. Selecting the role of the virtual machine

The step is displayed if you chose to use the application in Light Agent mode at step 2.

Specify the role of the virtual machine (server or workstation) on which you are installing Kaspersky Endpoint Security:

- Enter `yes` if you are using the virtual machine as a server.
- Enter `no` if you are using a virtual machine as a workstation.

The role of a virtual machine determines the license under which the application will be used on this virtual machine as well as the available functionality.

Step 6. Enabling VDI protection mode

The step is displayed if you chose to use the application in Light Agent mode at step 2.

VDI protection mode optimizes the operation of Kaspersky Endpoint Security on temporary virtual machines. If VDI protection mode is enabled, updates that require restarting the virtual machine are not installed. When receiving updates that require a restart, the Light Agent installed on the virtual machine sends a message to Kaspersky Security Center about the need to update the protected virtual machine template.

Specify `yes` if you want to enable VDI protection mode. This is recommended if you are installing Kaspersky Endpoint Security on a virtual machine template that will be used to create temporary virtual machines.

Specify `no` if you do not want to enable VDI protection mode. This is recommended if you are installing Kaspersky Endpoint Security on a persistent virtual machine or on a virtual machine template that will be used to create persistent virtual machines.

Step 7. Selecting the locale

At this step, the wizard displays the list of supported locales in RFC 3066 format.

Specify a locale as it is listed here. This locale is used for the following purposes:

- Localization of the texts of the End User License Agreement, Privacy Policy, and Kaspersky Security Network Statement, which are displayed during the installation.
- Localization of application events sent to Kaspersky Security Center.

The locale of the graphical interface and the application command line is taken from the `LANG` environment variable. If the application does not support this localization, it defaults to the English localization.

Step 8. Viewing the End User License Agreement and the Privacy Policy

At this step, read the End User License Agreement concluded between you and Kaspersky, and the Privacy Policy describing the processing and transfer of data.

Step 9. Accepting the End User License Agreement

After exiting viewing mode, enter one of the following values:

- `yes` (or `y`), if you accept the terms of the End User License Agreement.
- `no` (or `n`), if you do not accept the terms of the End User License Agreement.

If you did not accept the terms and conditions of the End User License Agreement, the Kaspersky Endpoint Security setup process is aborted.

Step 10.Accepting the Privacy Policy

After exiting viewing mode, enter one of the following values:

- `yes` (or `y`), if you accept the terms of the Privacy Policy.
- `no` (or `n`), if you do not accept the terms of the Privacy Policy.

If you did not accept the terms and conditions of the Privacy Policy, the Kaspersky Endpoint Security setup process is aborted.

Step 11.Using Kaspersky Security Network

At this step, accept or decline the terms of use of Kaspersky Security Network:

- Enter `yes` (or `y`) if you accept the terms and conditions of the Kaspersky Security Network Statement. This enables the extended KSN mode.
- Enter `no` (or `n`) if you do not accept the terms and conditions of the Kaspersky Security Network Statement.

The file ksn_license.<language ID> containing the text of the Kaspersky Security Network Statement is located in the directory /opt/kaspersky/kesl/doc/.

Refusal to participate in Kaspersky Security Network does not interrupt the initial configuration of Kaspersky Endpoint Security. You can enable, disable, or change the Kaspersky Security Network mode at any time.

If Kaspersky Security Network is enabled, the cloud mode is automatically enabled, in which Kaspersky Endpoint Security uses the lightweight version of malware databases.

Step 12. Removing users from privileged groups

This step is displayed if users are detected in the kesladmin and/or the keslaudit group.

Specify whether or not to remove users from the kesladmin and keslaudit privileged groups. Users included in the kesladmin and keslaudit groups receive privileged access to the application's functions.

Enter `yes` to remove all detected users from the kesladmin and/or keslaudit group. Users whose primary group is kesladmin or keslaudit will be moved to the nogroup group. If there is no nogroup group, the installation will fail and you will be prompted to manually remove users from privileged groups.

Enter `no` if you do not want the application to remove users from the privileged groups.

Step 13. Assigning the Administrator role to a user

At this step, the wizard prompts you to grant the administrator role (admin).

Enter the name of the user to whom you want to grant the administrator role. You need the Administrator role to manage application settings and task settings in the graphical interface of the application and on the command line without using the `sudo` command.

You can assign the administrator role to a user later, after completing the initial configuration.

Step 14. Configuring the system event interception mechanism

The application can use the interception mechanism based on the updatable kernel module if the operating system meets the requirements for its installation. If the operating system does not meet these requirements but supports the fanotify technology, the application uses fanotify to intercept system events. If the operating system does not support the fanotify technology, the application will compile and use a special kernel module to intercept system events for File Threat Protection. If all the necessary packages are installed, the compilation of the kernel module will start automatically when File Threat Protection is launched. If any dependencies are not found on the device, the Kaspersky Endpoint Security application suggests installing the relevant packages. If the package download fails, an error message will be displayed.

- Enter `yes` if you want to use the updatable kernel module.
- Enter `no` if you want to use fanotify.

If you select the updatable kernel module as the interception mechanism, specify the following settings:

- What the application does if the updatable kernel module fails to start:
  - Enter `yes` if you want the application to fall back to fanotify for system events interception if the updatable kernel module fails to start.
  - Enter `no` if you want the application to continue running without system event interception if the updatable kernel module fails to start.

    If the application does not use system event interception, real-time file scanning is not performed, and the protection level of the device is reduced.

- Application restart mode when switching to using the updatable kernel module. To run the module, the application must be restarted automatically or manually.

  We recommend automatically restarting the application to switch to using the updatable kernel module. Starting the updatable kernel module manually after restarting the application can lead to application errors.

Enter `yes` if you want to allow automatically restarting the application to run the module.

Step 15. Enabling automatic configuration of SELinux

This step is displayed if the SELinux access control system is installed in your operating system.

Enter `yes` to automatically configure SELinux for working with Kaspersky Endpoint Security. If the application is unable to configure SELinux automatically (for example, if the semanage utility is missing), the wizard displays an error message and prompts the user to configure SELinux manually.

Enter `no` if you do not want to perform automatic configuration of the SELinux system.

By default, the wizard suggests `yes`.

If necessary, you can manually configure SELinux to work with the application later, after the initial configuration of the application is complete.

Step 16. Configuring the update source

The step is displayed if you are installing Kaspersky Endpoint Security in Standard mode or EDR Agent mode.

Specify the update source for databases and application modules. The application databases contain descriptions of the threat signatures and methods of countering them. The application uses these records when searching and neutralizing threats. Kaspersky virus analysts regularly add new records about threats.

Enter one of the following values:

- `KLServers`: the application receives updates from one of the Kaspersky update servers.
- `SCServer`: the application downloads updates to the protected device from Kaspersky Security Center Administration Server installed in your organization. You can select this update source if you use Kaspersky Security Center for centralized administration of device protection in your organization.
- `Custom`: the application downloads updates from a custom source. You can specify the address of a custom update source as a local directory (for example, /home/databases) or a remote HTTP or HTTPS server (for example, http://example.com/databases/).

Step 17.Configuring proxy server settings

The step is displayed if you are installing Kaspersky Endpoint Security in Standard mode or EDR Agent mode.

If you use a proxy server for your internet connection, enter the address of your proxy server in one of the following formats:

- `[<connection protocol>://]<address of proxy server>:<port>`, if no authentication is required to connect to the proxy server;
- `[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, if authentication is required when connecting to the proxy server. When specifying an IPv6 address, enter it in square brackets.

> Connecting to a proxy server over HTTPS is not supported. When connecting via an HTTP proxy, we recommend to use a separate account that is not used to sign in to other systems. An HTTP proxy uses an insecure connection, and the account may be compromised.

If you do not use a proxy server, enter `no`.

By default, the application suggests `no`.

You can manage proxy server settings later, after completing the initial configuration.

Step 18. Starting an application database update

The step is displayed if you are installing Kaspersky Endpoint Security in Standard mode or EDR Agent mode.

At this step, the wizard offers to run the application database update task on the client device immediately after installation.

If you do not want to start to download the application databases, enter `no`.

By default, the wizard suggests `yes`.

If `yes` is selected, the application will be automatically restarted after the databases are updated.

> Kaspersky Endpoint Security protects the device only after the application databases are updated.

You can run the update task later, after completing the initial configuration.

Step 19. Enabling automatic application database update

The step is displayed if you are installing Kaspersky Endpoint Security in Standard mode or EDR Agent mode.

Enter `yes` to enable automatic application database update. By default, the application checks for available database updates every 60 minutes. If updates are available, the application downloads the updated databases.

Enter `no` if you do not want the application to automatically update the databases.

You can enable automatic database update later, after completing the initial configuration, by configuring the update task schedule.

Step 20. Application activation

The step is displayed if you are installing Kaspersky Endpoint Security in Standard mode or EDR Agent mode.

If you want to activate the application immediately after installation, enter an activation code or specify the full path to a key file.

> If no activation code or key file is specified, the application is activated using a trial key for one month.

You can activate the application later, after completing the initial configuration.

How to perform initial configuration in automatic mode

1. Create a configuration file that contains the initial configuration settings. You can copy the settings from the autoinstall.ini configuration file, which is used for remote installation of the application using Kaspersky Security Center, and make changes as necessary.

2. Specify the following required settings in the configuration file:

   - Accepting the End User License Agreement (EULA) and the Privacy Policy:

     ```
     EULA_AGREED=Yes
     PRIVACY_POLICY_AGREED=Yes
     ```

     You can read the terms and conditions of the End User License Agreement and the Privacy Policy in a license.<language ID> file included in the distribution kit of the application:

     > If you do not accept the terms and conditions of the End User License Agreement and the Privacy Policy, the installation process is aborted.

   - The Kaspersky Security Network application is used in standard mode by default.

     To use the application in EDR Agent mode, specify the following setting:

     ```
     ENDPOINT_AGENT_MODE=Yes
     ```

     To use the application in Light Agent mode, specify the following setting:

     ```
     KSVLA_MODE=Yes
     ```

   - Using Kaspersky Security Network. Accept or decline the terms of use of Kaspersky Security Network:

     ```
     USE_KSN=Yes|No
     ```

The file ksn_license.<language ID> containing the text of the Kaspersky Security Network Statement is located in the directory /opt/kaspersky/kesl/doc/. If you accept the terms and conditions of the Kaspersky Security Network Statement, extended KSN mode is enabled. You can enable, disable, or change the Kaspersky Security Network mode at any time.

> If Kaspersky Security Network is enabled, the cloud mode is automatically enabled, in which Kaspersky Endpoint Security uses the lightweight version of malware databases.

- Automatically removing users from the kesladmin and keslaudit privileged groups before installing the application:

  `GROUP_CLEAN=Yes|No`

3. Select the system event interception mechanism used by Kaspersky Endpoint Security. If you want to use the updatable kernel module to intercept system events, set the value:

   `INTERCEPTOR_MODE=UseUpdatableKernelModule`

   By default, the fanotify technology is used to intercept system events.

4. If you are installing the application in Standard mode or EDR Agent mode, specify the following settings:

   - Proxy server settings. If you use a proxy server for your internet connection, enter the address of your proxy server in one of the following formats:

     - `PROXY_SERVER=[<connection protocol>://]<address of proxy server>:<port>`, if no authentication is required to connect to the proxy server;

     - `PROXY_SERVER=[<connection protocol>://][<user name>:<password>@]<address of proxy server>:<port>`, if authentication is required when connecting to the proxy server. When specifying an IPv6 address, enter it in square brackets.

     > Connecting to a proxy server over HTTPS is not supported.

   - Install and use the graphical interface of the application:

     `USE_GUI=Yes|No`

5. If you are installing the application in Light Agent mode, specify the following settings:

   - Role of the protected virtual machine:

     - `SERVER_MODE=Yes`, if the protected virtual machine is used as a server.

     - `SERVER_MODE=No`, if the protected virtual machine is used as a workstation.

   - Enabling VDI protection mode to optimize application performance on temporary virtual machines. If you are installing the application on a virtual machine template from which temporary virtual machines will be created, set the value:

     `VDI_MODE=Yes`

6. Start the Initial Configuration Wizard:

```
/opt/kaspersky/kesl/bin/kesl-setup.pl --autoinstall=<initial configuration file>
```

Where `<initial configuration file>` is the path to the configuration file with the initial configuration settings.

When the Initial Configuration Wizard finishes and releases the console, the post-installation configuration of the application is complete.

```
Check return code
echo $?
```

If the command returns 0, the post-installation configuration of the application is completed successfully.

4 Application health check

As a result, the Kaspersky Endpoint Security application has been installed, activated, and the application databases have been updated. After installation, the application starts automatically. By default, the following components are enabled:

- File Threat Protection.
- Device Control.
- Behavior Detection.
- Web Threat Protection—only if one of the supported browsers is installed in the operating system and local management of Web Threat Protection settings is allowed on the device (a policy is not applied or the "lock" is not set in the policy properties).
- Network Threat Protection—only if the Network Threat Protection settings on the device are defined through a policy. Network Threat Protection is enabled in the policy properties by default. If locally configured settings are applied on the device, Network Threat Protection is disabled by default.

Checking the protection status of the device for Standard mode

```
To check the protection status of the device, run the following command:
kesl-control --app-info [--json]
```

Where `--json` means output data in JSON format. If you do not specify the `--json` option, settings will be output to the console.

Make sure that:

- The application is activated (the **Application license information** line).
- Application databases are up-to-date (the **Application databases loaded** and **Last release date of databases** lines).
- File Threat Protection is enabled (the **File Threat Protection** line).

- The **Application status** line displays `OK`.

  If the **Application status** line displays information about insufficient rights to system directories, check the permissions for the following directories locally on this device: /var/opt/kaspersky, /var/log/kaspersky, and /opt/kaspersky. Make sure that the owner is root and that only the owner has write access to these directories.

Checking the device protection status for EDR Agent mode

```
To check the protection status of the device, run the following command:

kesl-control --app-info [--json]
```

Where `--json` means output data in JSON format. If you do not specify the `--json` option, settings will be output to the console.

Make sure that:

- The application is activated (the **EDR Expert (on-premises) license information** line)
- Application databases are up-to-date (the **Application databases loaded** and **Last release date of databases** lines).
- The application is used in EDR Agent mode (the **Endpoint Detection and Response Agent mode** line).
- For the integrations that you configured in the policy, the "Available and running" status is displayed.
- The **Application status** line displays `OK`.

  If the **Application status** line displays information about insufficient rights to system directories, check the permissions for the following directories locally on this device: /var/opt/kaspersky, /var/log/kaspersky, and /opt/kaspersky. Make sure that the owner is root and that only the owner has write access to these directories.

Checking the device protection status for Light Agent mode

1. Run the following command:

   ```
   kesl-control --ksvla-info
   ```

   Make sure the application is used in Light Agent mode (the **Light Agent mode for protecting virtual environments** line).

2. If you have selected an Integration Server in the policy to detect SVMs available for connection, run the following command:

   ```
   kesl-control --viis-info
   ```

   Make sure that Light Agent is connected to the Integration Server (the **Status of connection to the Integration Server** line).

3. Run the following command:

   ```
   kesl-control --svm-info
   ```

   Make sure that Light Agent is connected to the SVM: information is displayed about the SVM to which a connection is established.

4. Run the following command:

```
kesl-control --app-info [--json]
```

Where `--json` means output data in JSON format. If you do not specify the `--json` option, settings will be output to the console.

Make sure that:

- The Light Agent receives information about the license that Kaspersky Security for Virtualization Light Agent is activated with (the **Application license information** line).
- Application databases are up-to-date (the **Application databases loaded** and **Last release date of databases** lines).
- The **Application status** line displays `OK`.

  If the **Application status** line displays information about insufficient rights to system directories, check the permissions for the following directories locally on this device: /var/opt/kaspersky, /var/log/kaspersky, and /opt/kaspersky. Make sure that the owner is root and that only the owner has write access to these directories.

Useful articles

What to do if tasks do not run or policies are not applied

What to do if the device has the status: "Invalid policy settings. Policy has not been applied."

Error: "Application is not supported by the current version of Kaspersky Security Center Web Console or application web plug-in is not installed"

Troubleshooting an issue when installing the GUI

Description of installation error codes

Errors following Kaspersky Endpoint Security installation

After you have installed Kaspersky Endpoint Security, you can go back to the deployment scenario and continue from the Additional configuration steps after installation in certain operating systems step.

Additional configuration steps after installation in certain operating systems

After preparing the environment for Kaspersky Endpoint Security installation and installing the application, additional configuration is required for some operating systems.

Manually configuring SELinux for working with the application

If your operating system uses the SELinux access control system in `Enforcing` mode, it is automatically configured to work with the application by default during installation.

If the application is unable to configure SELinux automatically (for example, if the semanage utility is missing), the wizard displays an error message and prompts the user to configure SELinux manually. In this case, or if you declined automatic configuration, after completing the initial configuration of the application, manually configure the SELinux system to work with the Kaspersky Endpoint Security application.

This configuration requires root privileges.

To manually configure SELinux to work with the application:

1. Switch SELinux to permissive mode:

   - If SELinux is enabled, run the following command:

     ```
     setenforce Permissive
     ```

   - If SELinux is disabled, set `SELINUX=permissive` in the /etc/selinux/config configuration file and restart the operating system.

2. Make sure the semanage utility is installed on the system. If the utility is not installed, install the policycoreutils-python or policycoreutils-python-utils package, depending on the package manager.

3. If you use a custom SELinux policy rather than the default 'targeted' policy, assign a label for each of the original Kaspersky Endpoint Security executable files in accordance with your SELinux policy.

   ```
   semanage fcontext -a -t bin_t <executable file>
   restorecon -v <executable file>
   ```

   Where `<executable file>` is:

   - /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/shared/kesl
   - /var/opt/kaspersky/kesl/<build number_*>/opt/kaspersky/kesl/bin/response

4. Run the following tasks:

   Run the File Threat Protection task

   ```
   kesl-control --start-task 1
   ```

   Run the Critical Areas Scan task

   ```
   kesl-control --start-task 4 -W
   ```

   We recommend running all the Kaspersky Endpoint Security tasks that you intend to run in the future.

5. Start the graphical user interface if you plan to use it.

6. Make sure there are no errors in the audit.log file.

```
View the audit.log file

grep kesl /var/log/audit/audit.log
```

7. If there are errors in the audit.log file, create and download a new rule module based on the blocking records in order to fix the errors, then relaunch all the tasks that you plan to run in the future.

```
Create and load a new rules module based on blocking records:

grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

> If new audit messages related to Kaspersky Endpoint Security appear, the file with the rule module file must be updated.

8. Switch SELinux to enforcing mode.

```
setenforce Enforcing
```

> If you use a custom SELinux policy, manually assign a label to Kaspersky Endpoint Security source executable files after installing application updates (follow steps 1, 3–8).

You can find more information in the documentation for your operating system.

Configuring SELinux for response actions

If you plan to use SELinux in the `Enforcing` mode on your operating system, then to perform response actions when integrating with Detection and Response solutions, you need to additionally manage SELinux settings.

> This SELinux configuration requires root privileges.

To configure SELinux for response actions:

1. Switch SELinux to permissive mode:

   - If SELinux is enabled, run the following command:

     ```
     Switch SELinux to permissive mode

     setenforce Permissive
     ```

   - If SELinux is disabled, set `SELINUX=permissive` in the /etc/selinux/config configuration file and restart the operating system.

2. Make sure the semanage utility is installed on the system. If the utility is not installed, install the policycoreutils-python or policycoreutils-python-utils package, depending on the package manager.

3. Run all tasks to perform the response actions that you want to use as part of integration with Detection and Response solutions.

4. To collect forensics using the Get memory dump task and the Get process memory dump task, in SELinux, allow the Kaspersky Endpoint Security application to gain access to the SMB servers specified in the tasks.

5. Make sure there are no errors in the audit.log file.

```
View the audit.log file

grep kesl /var/log/audit/audit.log
```

6. If any errors are present in the audit.log file, create and load a new rules module based on blocking records to fix the errors, then run the response actions tasks again.

```
Create and load a new rules module based on blocking records:

grep kesl /var/log/audit/audit.log | audit2allow -M kesl
semodule -i kesl.pp
```

7. Switch SELinux to enforcing mode.

```
setenforce Enforcing
```

Configuring the application launch in the OSnova operating system

After installing the application, follow these steps to configure the launch of the application and its graphical interface:

1. Open the `/etc/NESS/systemd/kesl.service.config` file and set `NESSCTX_MODIFY="t+ADDEQUSOCK,OMIT,OMIT_PID,SSUID_SAVE_CTX_PERMANENT"`.

2. Open the `/etc/sysctl.d/30-disable-ptrace.conf` file and set `kernel.yama.ptrace_scope=0`. Other values of the `kernel.yama.ptrace_scope` parameter may affect the operation of the Kaspersky Endpoint Security application; for more details, see the Known issues and limitations section.

3. If you want to run a scan of process memory and kernel memory, you need to disable the mprotect (or PaX) memory protection mechanism in the kernel. To do this, add the `mprotect=off` option to the command line of the kernel. For more details, please refer to the OSnova documentation.

4. Restart the operating system.

Configuring the launch of the application on ALT SP in closed software environment mode

After installing the application, follow these steps to launch of the application:

1. Assign the inheritance of the kesl group and directory permissions for the updatable components of Kaspersky Endpoint Security:

```
cd /var/opt/kaspersky/kesl/<build number_*>/var/opt/kaspersky/kesl/private
chown -R root:kesl updates/
find updates -type d -exec chmod g+s {} \;
cd /opt/kaspersky/kesl/lib64
chown -R root:kesl updatable_modules/
find updatable_modules -type d -exec chmod g+s {} \;
cd /var/opt/kaspersky/kesl/common/
chown -R root:kesl temp/
find temp -type d -exec chmod g+s {} \;
```

2. Assign the inheritance of the kesl group and directory permissions for the updatable components of the Network Agent:

```
cd /var/opt/kaspersky/
chown -R root:kesl klnagent/
find klnagent/ -type d -exec chmod g+s {} \;
cd /opt/kaspersky/
chown -R root:kesl klnagent64/
find klnagent64/ -type d -exec chmod g+s {} \;
```

3. Enable the closed software environment mode by initiating the signing of the system:

```
integrity-applier -i -A
```

4. Make sure the IMA subsystem is activated:

```
cat /proc/cmdline
```

The output of the command should contain the lines `lsm=integrity ima_hash=sha512 ima_appraise=enforce`.

5. Run the database update task:

```
kesl-control --start 6 -W
```

If the output of the database update task contains an *EventType=BasesApplied* event, it means the database update was performed correctly.

6. Restart the application:

```
systemctl restart kesl
```

Migration scenario to Kaspersky Security Center for Linux using the fast installation script

This scenario includes examples for the following use cases of migrating the solution with data to a new Administration Server device:

- Migrating from Kaspersky Security Center Windows (MS SQL and PostgreSQL) to Kaspersky Security Center Linux (PostgreSQL).
- Migrating Kaspersky Security Center Linux (PostgreSQL) for hardware replacement.

The new Administration Server is deployed using the fast installation script.

Other ways to transfer data are described in the section on migrating to Kaspersky Security Center Linux.

1 Prerequisites for creating a backup copy

This step contains instructions for preparing a previously configured Administration Server for subsequent migration to a new Kaspersky Security Center Linux Administration Server. The preparation process involves the following steps:

1. Checking the version of the Administration Server to create a backup copy compatible with Kaspersky Security Center Linux.

   All current versions of **Kaspersky Security Center Linux** support data migration with an upgrade of the application to a newer version. Backup copies can be created and restored only within the same DBMS type.

   For **Kaspersky Security Center Windows**, you need to check the version of the Administration Server in **Properties** → **General** → **Version**. If the version is older than 15.1.0.22239, upgrade Kaspersky Security Center Windows to the latest version.

   Upgrading Kaspersky Security Center for Windows to the latest version.

   1. On the Kaspersky website, download the distribution package matching the localization language of the installed Administration Server: `Version 15.1.0.22239 | Windows | Full distributive`.

      The executable file is saved to the **Downloads** folder with the following name: `ksc_15.1_<build number>_full_<language>.exe`.

   2. Copy the distribution package to the Administration Server.

   3. Run the `ksc_15.1_<build number>_full_<language>.exe` executable file as administrator.

   4. In the displayed window, click the **Install Kaspersky Security Center** link.

      The Administration Server setup wizard starts.

   5. Review the terms of the End User License Agreement and Privacy Policy. If you agree with all terms and conditions of the End User License Agreement and the Privacy Policy, in the **I confirm that I have fully read, understand, and accept the terms and conditions of the following** section, select the following check boxes:

      - **The terms and conditions of this EULA**.
      - **Privacy Policy describing the handling of data**.

   6. Select **Upgrade Administration Server and web-based console (recommended)** and go to the next step.

   7. Create a new backup copy, select the **I want to create a backup copy of data** option, and follow the steps of the backup wizard.

   8. Click **Upgrade**.

   9. During the upgrade, in the Web Console installation wizard, confirm all steps to upgrade the version.

      The installation of the Administration Server upgrade will take some time. After the installation wizard finishes, the Administration Console may not accept connections until the database initialization is complete.

   10. Wait until the upgrade is complete.

2. Verification of compliance with the requirements for the Administration Server certificate.

Before creating a backup copy, you need to make sure that the certificate contains the Subject Alternative Name (SAN). If it does not, make sure to replace the certificate because otherwise you will not be able to log in to the Web Console after restoring from a backup.

To verify that the certificate includes the subject alternative name:

- For devices running Windows:

  a. In the Administration Console, select the Administration Server which you want to check.

  b. In the context menu, select **Properties** → **General** → **View Administration Server certificate**.

  c. This opens a window; in that window, check the value of the **Subject Alternative Name** item.

- For a Linux device, run the following command:

```
sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
```

Make sure that the subject alternative name contains the domain name (DNS) of the Administration Server device.

If the value contains only an external IP address without a domain name (DNS), or the value is missing altogether, manually replace the certificate with one that meets the requirements of Kaspersky Security Center Linux. Replace the common certificate of the Administration Server using the klsetsrvcert utility.

Replacing the common certificate of the Administration Server using the klsetsrvcert utility

1. Create a new certificate with a postponed start date on devices by running the following command:

   - For Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -t CR -g "
<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   - For Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -t CR -g "<oldksc.example.internal>" -o "RsaKeyLen:2048"
```

   where `"<oldksc.example.internal>"` is the FQDN for the connection to the Administration Server.

   > Do not use an IP address for this value.

2. Set the start date for the new certificate on all devices by running the following command:

   - For Kaspersky Security Center Windows:

```
"%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\klsetsrvcert.exe" -f "DD-MM-YYYY hh:mm"
```

   - For Kaspersky Security Center Linux:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert -f "DD-MM-YYYY hh:mm"
```

where `"DD-MM-YYYY hh:mm"` is a date at least 30 days after the current date. By default, the distribution period for a new certificate (`CR`) is 90 days.

> When the set time arrives, you will need to reinstall the Web Console to restore access to it and update its certificate.

3. If necessary, after migrating to the new Administration Server, run the klmover utility to restore the connection of devices to the Administration Server. You may need to start this utility if a device has stayed turned off for the entire certificate distribution period or if it has never connected to the Administration Server.

2 Creating a backup copy of the previous Administration Server installation

Creating a backup copy of Kaspersky Security Center Windows

1. From **Start menu** → **Kaspersky Security Center** → **Kaspersky Backup Utility**, run the `klbackup.exe` utility that is located in the Kaspersky Security Center Linux installation folder.

   The Setup Wizard starts. On Microsoft Windows in Server Core mode, use the console version of the klbackup utility.

2. At the first step, select **Perform backup of Administration Server data**.

3. At the **Backup settings** step:

   a. Click the **Browse** button and create a new folder to save the backup copy separately from the default directory, for example `C:\kscbackups`.

   b. If you are using Microsoft SQL Server, select the **Migrate database** → **Migrate to Postgres** option to use it with the fast installation script. When deploying Kaspersky Security Center Linux using the standard method, you can also migrate data to a MySQL/MariaDB database.

   c. Set a password for the backup copy to protect it against unauthorized access to data.

4. Wait for the backup copy to be created and exit the utility.

A new subdirectory with the timestamp of the backup is created in the specified directory.

Creating a backup copy of Kaspersky Security Center Linux

1. On the Administration Server device, run the following command on the command line:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path /root/kscbackups -use_ts
```

2. Wait until the backup process finishes.

A new subdirectory with the timestamp of the backup is created in the directory specified in the `-path` option.

After creating a backup copy of your old Administration Server, put the Administration Server device out of service.

Putting the Administration Server device out of service

1. Copy the obtained backup copy for data migration to the administrator's device.
2. Shut down the operating system of the Administration Server.
3. Unplug the network adapter from the corporate network.
4. Free up the IP address of the device if you plan to reuse it for the new installation of Kaspersky Security Center Linux.
5. Make sure the device is completely powered off.

> The old Administration Server remaining on the network may cause device management faults and disrupt the Web Console login process of the new Administration Server, as well as make the Network Agent installation task start with a connection to the old server.

3 Initial deployment of Kaspersky Security Center Linux using the fast installation script

This guide describes the initial deployment of a Kaspersky Security Center Linux instance using the fast installation script.

Special considerations:

- All components of Kaspersky Security Center are installed on the same device as the Administration Server.
- The operating system of the Administration Server must be of the following:
  - Astra Linux Special Edition RUSB.10015-01 (operational update 1.8.5) with PostgreSQL 15
  - Ubuntu Server 26.04 LTS with PostgreSQL 18
  - CentOS Stream 10 with PostgreSQL 18
  - RED OS 8.0 with PostgreSQL 16
- The fast installation script automates only configuration and installation of the Kaspersky Security Center application. The administrator must take steps to configure the name of the Administration Server device in the operating system, network adapters and security firewalls at the operating system level, and the hardware.

Initial deployment of an instance of Kaspersky Security Center Linux using the fast installation script involves the following steps:

1. Preparing for deployment

Before proceeding with the installation steps, you must prepare:

- An installation disk image of the operating system a repository of application packages.
- An authenticator application for two-factor authentication (2FA) when logging in to the Web Console.

- A new FQDN (for example, *ksclinux.example.com*). You can use your own script to assign the previous FQDN to the new server during installation if you have sufficient experience configuring solutions. In this case, in Step 5, "Configuring the application after restoring from a backup copy", skip Step 4. Restoring the connection of managed devices to the FQDN of the previous Administration Server

- An administrator's device with a browser for downloading distributions and managing the Web Console over the internet.

- Ensure the availability of DNS and a time server (NTP) for application components.

- Depending on your scenario, release the previous IP address if it was used to connect managed devices.

- Configure network equipment and the proxy server in accordance with the requirements:

  - Ports for communication between application components.

  - Access to Kaspersky servers.

  - Recommendations of the Hardening guide.

2. Sizing and configuring the operating system

1. Configure the equipment in accordance with the number of devices that the Administration Server will manage.

   Each sizing calculation takes into account available resources for Kaspersky applications. The calculation accounts for the Administration Server, Network Agent, DBMS, Web Console server, and Kaspersky Endpoint Security for Linux all working on the same device. However, the calculation does not account for the storage of backup copies of the Administration Server.

   > Use an external file share as a mount point for storing backup copies on a separate device or increase the free hard disk space requirement taking into account the storage of backups.

   We recommend adding 4–6 GB of RAM and 20 GB of free hard disk space for the operating system.

   Sizing the device depending on the number of managed devices:

   - **S** (up to 1000 devices): 8 CPU cores, 16 GB of RAM, 70 GB of free hard disk space for the `/var` directory, 300 IOPS or more.

   - **M** (up to 10,000 devices): 12 CPU cores, 24 GB of RAM, 340 GB of free hard disk space for the `/var` directory, 300 IOPS or more.

   - **L** (up to 30,000 devices): 20 CPU cores, 40 GB of RAM, 490 GB of free hard disk space for the `/var` directory, 300 IOPS or more.

   - **XL** (up to 50,000 devices): 28 CPU cores, 54 GB of RAM, 640 GB of free hard disk space for the `/var` directory, 300 IOPS or more.

2. Prepare the hardware for the Kaspersky Security Center server in accordance with the selected specifications.

3. Install the operating system on the Kaspersky Security Center server.

   During installation, enable the **SSH remote connection tools** option if you intend to manage the Administration Server device remotely on the command line.

Astra Linux must be installed with the **Mandatory Access Control** option disabled. Also, for the Kaspersky Endpoint Security for Linux to work correctly, disable the **Block ptrace tracing** option.

4. Check free disk space for the `/var` directory if it is mounted separately, or for the root directory `/`.

   Examples for an M configuration:

   Astra Linux

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                 Size  Used Avail Use% Mounted on
   /dev/mapper/astra48242-01  406G  8,0G 377G    3% /
   <...>
   ```

   Ubuntu

   ```
   administrator@ksclinux:~$ df -h
   Filesystem                        Size  Used Avail Use% Mounted on
   /dev/mapper/ubuntu--vg-ubuntu--lv  406G   11G  374G   3% /
   <...>
   ```

5. Configure the IP address from the previous Administration Server on the new server if an IP address was used to connect managed devices.

Video: configuring the operating system

3. Downloading distribution files

1. Download the distribution packages for the desired locale from the Kaspersky website and save these in a separate directory (for example, *kscdistr*).

   For Ubuntu and Astra Linux

   - Distribution package of the Administration Server in deb format:

     `Version 16.3.0.1207 | Debian x64 | Administration server`

   - Distribution package of the Web Console in deb format:

     `Version 16.3.0.1207 | Debian x64 | Web console`

   - Fast installation script:

     `Version 16.3.0.1207 | Linux | KSC installation script`

For CentOS and RED OS

- Distribution package of the Administration Server in rpm format:

  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Administration server`

- Distribution package of the Web Console in rpm format:

  `Version 16.3.0.1207 | Red Hat Enterprise Linux x64 | Web console`

- Fast installation script:

  `Version 16.3.0.1207 | Linux | KSC installation script`

2. To make it possible for Kaspersky applications to work in the closed software environment mode of Astra Linux, download the public key file, kaspersky_astra_pub_key.gpg.

3. Copy the downloaded files to the new Kaspersky Security Center Administration Server device using removable media or over the network.

   The following are the actions for copying over the network using the command line.

   > Whether you can use the scp utility to copy the files depends on whether an SSH service is running in the operating system of the Administration Server device, as well as the security policy of your organization.

   a. On the command line, use the cd command to change to the directory one level above the *kscdistr* directory, for example:

   For Linux

   ```
   cd /home/administrator/Desktop
   ```

   For Windows

   ```
   cd C:\Users\Administrator\Downloads
   ```

   b. Copy the distribution files over the network using the scp utility:

   ```
   scp -r <kscdistr> <administrator>@<ksclinux.example.com>:
   ```

   where:

   `<kscdistr>` is the local directory with downloaded distribution packages of Kaspersky Security Center.

   `<administrator>` is a superuser on the new Administration Server that is authorized to use an SSH connection.

   `<ksclinux.example.com>` is the FQDN address of the new Administration Server.

   The files are copied to the root of the home directory of the specified user.

4. Configuring installation settings

1. On the new Administration Server device, log in as a superuser and open a terminal.

2. Go to the directory with the copied distribution packages.

Example

```
cd ~/kscdistr
```

3. Extract the archive of the fast installation script into the current directory with distribution files.

Example

```
tar -xf ./ksc_fast_install.tar.gz
```

4. Check if all files are present by running the following command:

```
ls -la
```

Example of the ls -la command output

```
administrator@ksclinux:~$ ls -la
drwxr-xr-x  3 administrator administrator      4096 jul 17 20:32 .
drwx------ 17 administrator administrator      4096 jul 17 17:54 ..
-rw-r--r--  1 administrator administrator       493 apr 20  2023 kaspersky_astra_pub_key.gpg
-rw-r--r--  1 administrator administrator 199128488 jul 10 21:38 ksc64_16.3.0-1207_amd64.deb
-rwxr-xr--  1 administrator administrator    143288 jul 22 17:22 ksc_fast_install.py
-rw-r--r--  1 administrator administrator 158144492 jul 10 21:37 ksc-web-console-16.3.12907.x86_64.deb
-rw-r--r--  1 administrator administrator     15561 jul 22 23:17 nwc_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 nwc_license.txt.sha256
-rw-r--r--  1 administrator administrator       493 jul 22 17:22 params.txt
-rw-r--r--  1 administrator administrator     70869 jul 22 23:17 server_license.txt
-rw-r--r--  1 administrator administrator        64 jul 22 23:17 server_license.txt.sha256
```

5. In the directory with distributions, open the text file with settings of the installation script for editing, for example:

```
nano ./params.txt
```

6. Set the previously prepared values and remove the first comment character (#) in the relevant lines, or add new lines with the following values:

   - Equipment sizing (values for the S/M/L/XL configurations).

     Example

     ```
     klfi_netsize=S
     ```

   - FQDN address of the Administration Server in two settings in the file.

     ```
     klfi_klserver_address=ksclinux.example.com
     ```

     ```
     klfi_kliam_address=ksclinux.example.com
     ```

The language of the installed Administration Server depends on the locale of the downloaded distribution package.

7. Check if the FQDN of the Administration Server is being resolved correctly to the loopback IP address in the operating system of the new Administration Server. To do so:

   a. Run the `ping` command with the address of the new Administration Server.

   Example of successfully getting a loopback IP address

   ```
   administrator@ksclinux:~$ ping ksclinux.example.com
   ping ksclinux.example.com
   PING ksclinux.example.com (127.0.1.1) 56(84) bytes of data.
   64 bytes from ksclinux.example.com (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
   ```

   b. Add the address of the Administration Server to the `/etc/hosts` file of the operating system on the new Administration Server, if an address was not obtained or an external IP address was obtained.

   To do so:

   - Open the `/etc/hosts` file for editing by running the following command:

     ```
     sudo nano /etc/hosts
     ```

   - Enter the server address as the FQDN of the Administration Server device, for example:

     ```
     127.0.0.1       localhost
     127.0.1.1       ksclinux.example.com ksclinux
     <...>
     ```

On managed devices, the FQDN of the Administration Server must be resolved to the external IP address of the server. Make sure that records on DNS servers are set up correctly.

5. Starting the fast installation script

To run the fast installation script:

1. After restarting the device, go back to the directory with distribution packages:

   ```
   cd ~/kscdistr
   ```

2. Make the file executable by running the following command:

   ```
   chmod +x ./ksc_fast_install.py
   ```

3. Read the End User License Agreements in the language of your localization before running the script because the fast installation script itself is available only in English.

4. Connect network package repositories to the operating system or the operating system installation disk image so that packages can be downloaded during installation.

5. Run the fast installation script:

```
sudo ./ksc_fast_install.py
```

6. Follow the steps of the installation wizard.

> If the script falsely claims that you do not have enough RAM at the resource check step, disable dynamic RAM allocation during installation.

7. Wait for the installation to complete. From the text output of the script, save the user name (`User`) and password (`Pass`) for the Web Console.

Example

```
[+] Creating KSC user 'kscadmin' ...
[+] An internal user has been created:
[+]     User: kscadmin
[+]     Pass: ############
[!] If the password is lost, you must create a user by running the command:
        /opt/kaspersky/ksc64/sbin/kladduser -n <user>
[+] OK
[+] Success
```

Video: running the fast installation script for Ubuntu

6. Logging in to the Web Console for the first time

1. In a browser, open the Web Console address: `https://<FQDN>:8080`

   where `<FQDN>` is the Administration Server address from the installation script settings, for example, *https://ksclinux.example.com:8080*.

2. Log in to the Web Console with the user name and password from the script output.

3. Configure the authenticator application:

   a. Copy the secret key for getting one-time confirmation codes to the application or scan the QR code from the Web Console authentication wizard.

   b. Enter the generated confirmation code to authenticate and log in to the Web Console.

4. Review and confirm the Hardening Guide.

5. Configure the Administration Server in the Initial Configuration Wizard if you do not intend to restore the data of the Administration Server from a backup copy.

4 Restoring a backup copy of the Administration Server

In scenarios of migration from Kaspersky Security Center Windows or migration of Kaspersky Security Center Linux data to new hardware, you may need to restore data from a backup copy created in the old installation of the Administration Server.

> The PostgreSQL version on the new server must at least match the version in the backup copy.

Skip this step if you do not need to restore data.

If a backup copy has not been created before:

- Create a backup copy of the old Administration Server installation with the PostgreSQL data format type.
- Install a new Kaspersky Security Center Linux server and log in to the Web Console for the first time.

Restoring Administration Server from a backup copy involves the following steps:

1. Placing the backup copy on the Administration Server

Place the backup copy of the old Administration Server on the new Administration Server device using removable media or the network.

To copy the backup copy to the Administration Server over the network:

> Whether you can use the scp utility to copy the files depends on whether an SSH service is running in the operating system of the Administration Server device, as well as the security policy of your organization.

1. On the command line, use the *cd* command to navigate to the directory containing the backup files for the previous Administration Server, for example:

   Windows
   ```
   cd C:\kscbackups
   ```

   Linux
   ```
   cd /root/kscbackups
   ```

2. Copy the directory with the backup files using the scp utility:

   ```
   scp -r <klbackup202x-xx-xx> <administrator>@<ksclinux.example.com>:
   ```

   where:

`<klbackup202x-xx-xx>` is the directory in which the backup files are stored.

`<administrator>` is a superuser on the new Administration Server that is authorized to use an SSH connection.

`<ksclinux.example.com>` is the FQDN address of the new Administration Server.

The directory with the backup copy is copied to the home directory of the specified user.

2. Procedure for restoring from backup

1. On the new Administration Server device, open the terminal.

2. While restoring data from a backup copy, grant PostgreSQL superuser rights to the standard klserver and kliam accounts that the Administration Server uses for connection to the database:

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH SUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH SUPERUSER;"
```

3. Use the klbackup utility to initiate data restoration from the backup copy of the old Administration Server:

```
sudo /opt/kaspersky/ksc64/sbin/klbackup -path </home/administrator/klbackup202x-xx-xx> -restore
```

where `</home/administrator/klbackup202x-xx-xx>` is the full path to the directory with the backup files.

4. If no password has been set for the backup, press **Enter** without entering a password when prompted for a password for the backup.

5. Wait until the utility finishes.

   Large installations can take a long time.

6. Restore the original permissions for the PostgreSQL accounts that the Administration Server uses to connect to the database.

```
sudo -i -u postgres psql -c "ALTER ROLE klserver WITH NOSUPERUSER;"
```

```
sudo -i -u postgres psql -c "ALTER ROLE kliam WITH NOSUPERUSER;"
```

5 Configuring the application after restoring from a backup copy

Skip this step if you did not restore data from a backup copy.

Configuring the application after restoring from a backup copy involves the following steps:

1. Restoring the Web Console

1. Get the address of the old server from the IAM Server configuration file:

```
sudo grep "ksc_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Example

```
ksc_address: "oldksc.example.internal"
```

2. Check if the FQDN of the old Administration Server is being resolved correctly to the loopback IP address of the new Administration Server. To do so:

   a. Run the `ping` command with the address of the old Administration Server.

   Example of successfully getting a loopback IP address

```
administrator@ksclinux:~$ ping oldksc.example.internal
ping oldksc.example.internal
PING ksclinux (127.0.1.1) 56(84) bytes of data.
64 bytes from ksclinux (127.0.1.1): icmp_seq=1 ttl=64 time=0.037 ms
```

   b. Add the address of the Administration Server to the `/etc/hosts` file of the operating system on the new Administration Server, if an address was not obtained or an external IP address was obtained. To do so:

   - Open the /etc/hosts file for editing:

```
sudo nano /etc/hosts
```

   - Enter the name of the old server as an additional alias for the Administration Server device address.

   Example

```
127.0.0.1       localhost
127.0.1.1       ksclinux.example.com ksclinux oldksc.example.internal
<...>
```

3. Reinstall the Web Console:

   a. Uninstall the local Web Console server:

   Depending on your Kaspersky Security Center Linux distribution package, run one of the following commands:

   - On a Debian-based OS:

```
sudo apt remove ksc-web-console -y
```

   - On a device running an operating system based on Red Hat Enterprise Linux:

```
sudo dnf remove ksc-web-console -y
```

b. Install the Web Console package from the directory with distribution packages:

- On a Debian-based OS:

```
sudo apt install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.deb -y
```

- On a device running an operating system based on Red Hat Enterprise Linux:

```
sudo dnf install ~/kscdistr/ksc-web-console-16.3.12907.x86_64.rpm -y
```

2. Restoring the access of the kscadmin user when migrating from Kaspersky Security Center Windows

The user database has been overwritten; re-create the kscadmin user and configure two-factor authentication.

1. Open the terminal in the operating system of the Administration Server device and run the following command to create a user:

```
sudo /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin
```

After pressing **Enter**, enter a password, then re-enter it.

2. In a browser, open the Web Console address:

```
https://<FQDN>:8080
```

where `<FQDN>` is the Administration Server address from the installation script settings, for example, *https://ksclinux.example.com:8080*.

3. Use the created user name and password to log in to the Web Console.

4. Configure the authenticator application. To do so:

   a. Delete the old kscadmin user profile from the authenticator application before restoring the backup copy of the Administration Server.

   b. Copy the secret key for getting one-time confirmation codes to the application or scan the QR code from the Web Console authentication wizard.

   c. Enter the generated confirmation code to authenticate and log in to the Web Console.

3. Testing the Administration Server

1. Verify that the Web Console interface works properly when logged in as kscadmin and other users.

2. Successively run the following tasks:

   - Download updates to the Administration Server repository
   - Administration Server maintenance
   - Administration Server data backup

Replace the Windows paths in the settings of the tasks with Linux directories on the new Administration Server, or delete the tasks and configure them from scratch.

3. Check the results of the tasks and, if necessary, make changes to the settings of the tasks, management policies and Administration Server settings.

4. Restoring the connection of managed devices to the FQDN of the previous Administration Server

If you have assigned a new FQDN to the new Administration Server (for example, ksclinux.example.com), add one of the following types of DNS records:

- A CNAME record matching the old name of the Administration Server with the new name of the Administration Server.

  For details on how to configure the necessary records, refer to the documentation of your DNS server.

- A and AAAA records for the previous Administration Server address, pointing to the new IP address of the Administration Server.

  For a DNS service based on Windows Server, run the commands using the values applicable to your infrastructure.

To add a DNS A record for a DNS service based on Windows Server, run the commands using the values applicable to your infrastructure:

1. Connect to your DNS server.

2. Open PowerShell and get the IP address from the existing A record by running the following command:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

3. Change the IP address in the A record by running the following commands:

```
$OldKSC = Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration
server>"
```

```
$NewKSC = $OldKSC.Clone()
```

```
$NewKSC.RecordData.IPv4Address = [System.Net.IPAddress]::parse('<IP-address of the administration server>')
```

```
Set-DnsServerResourceRecord -OldInputObject $OldKSC -NewInputObject $NewKSC -ZoneName "<zone name>"
```

4. Verify that the IP address in the A record has been updated by running the following command:

```
Get-DnsServerResourceRecord -ZoneName "<zone name>" -RRType A -Name "<name of the administration server>"
```

   The output of the command includes the IP address of the Kaspersky Security Center Linux Administration Server. Managed devices will reconnect after the local DNS cache is updated.

6 Configuring anti-virus protection of the Administration Server

To comply with the recommendations of the Hardening Guide in terms of providing the Administration Server with anti-virus protection, install Kaspersky applications on the Administration Server and configure management policies. To deploy Kaspersky Endpoint Security for Linux, refer to the deployment guide.

Installation and configuration consist of the following steps:

1. Creating a separate administration group

1. In the main window of the Web Console, select **Asset management** → **Hierarchy of groups**.
2. Select the check box next to the **Managed devices** group.
3. Click **Add**.
4. In the displayed window, specify a name for the new group (for example, *kscserver*) and confirm its creation by clicking the **Add** button.

2. Creating a policy for the Network Agent without inheritance of settings

1. In the main window of the Web Console, go to the **Asset management** → **Policies** section.
2. Click the **Add** button.
3. In the New policy wizard, select the **Kaspersky Security Center Network Agent** application and click **Next**.
4. Disable the **Inherit settings from parent policy** option and click **Save**.

3. Installing the Kaspersky Endpoint Security for Linux administration plug-in from Kaspersky Security Center or manually

You can install the Kaspersky Endpoint Security for Linux administration plug-in in the following ways:

- Installing from the list of available distribution packages in the Web Console.
- Installing manually from a file.

To install the Kaspersky Endpoint Security administration plug-in from the list of available distribution packages in the Web Console:

1. In the main window of the Web Console, select **Settings** → **Web plug-ins**.

   A list of installed web plug-ins opens.

2. Click the **Add** button.

   This opens the list of available management plug-ins. The list is updated automatically after new versions of web plug-ins are released.

3. In the list of available plug-ins, select the latest available version of the Kaspersky Endpoint Security for Linux web plug-in.

4. In the window that opens with a description of the web plug-in, click the **Install plug-in** button.

5. Wait for the installation to complete and click **OK** in the information window.

The new plug-in will be displayed in the list of installed web plug-ins.

Video: Installing the management web plug-in using the wizard

To install the Kaspersky Endpoint Security management plug-in manually from a file:

1. Download the archive with the Web Plug-in from the application download page in the Kaspersky Endpoint Security for Linux section: **Application Control Plug-in** → **Web console Plug-in**.

2. Unpack the downloaded archive locally.

3. In the main window of the Web Console, select **Settings** → **Web plug-ins**.

   A list of installed web plug-ins opens.

4. Click the **Add from file** button.

5. This opens a window; in that window, specify the path to the plugin.zip file and the path to the signature.txt file.

   The files are located in the folder to which you unpacked the archive with the Web Plug-in.

6. Click the **Add** button.

7. Wait for the installation to complete and click **OK** in the information window.

The new plug-in will be displayed in the list of installed web plug-ins (**Settings** → **Web Plug-ins**).

Video: Installing the management web plug-in in isolated networks

4. Creating a policy for Kaspersky Endpoint Security for Linux without inheritance of settings

When using Kaspersky Endpoint Security for Linux together with Kaspersky Security Center Linux, you need to manage the policy settings in accordance with the recommendations of Kaspersky experts.

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Select an administration group for the Administration Server.
3. Click **Add**.

   The Policy Wizard starts.
4. In the displayed window, select Kaspersky Endpoint Security for Linux from the list.
5. Specify **Standard mode or Endpoint Detection and Response Agent mode** of the Kaspersky Endpoint Security for Linux application.
6. Decide whether you want to participate in Kaspersky Security Network.
7. Review the optimization recommendations for managed devices.
8. In the name of the policy, indicate that the policy belongs to the Administration Server.
9. Disable the **Inheritance from parent policy** option.
10. Save your changes.

Video: creating a policy

5. Creating the Update group task for Kaspersky Endpoint Security for Linux

1. In the main window of the Web Console, select the **Tasks** section.
2. Select an administration group for the Administration Server.
3. Click **Add**.

   The Task Wizard starts.
4. In the displayed window, select Kaspersky Endpoint Security for Linux from the list.
5. Specify the *Update* task type and go through the next steps without changing the settings.

   The task properties window opens.
6. In the **Application settings** → **Sources of updates** section, enable the Kaspersky Security Center source and raise its priority.

In an isolated network, use the Kaspersky Update Utility to create a repository for update tasks.

Video: configuring centralized database updates

6. Adding a license key to the store of the Administration Server with automatic key distribution functionality

1. In the main Kaspersky Security Center Web Console window, go to the **Licenses** section.
2. Click **Add**.
3. Specify the **Activation code** option and click **Send**.

   In an isolated network, use a key file that you can request using the https://keyfile.kaspersky.com/en-US service.
4. In the list of licenses, click the name of the license.
5. Select the **Automatically distribute license key to managed devices** check box.
6. Save your changes.

Video: Activating the application with an activation code

Video: Activating the application with a key file

7. Creating installation packages for Network Agent and Kaspersky Endpoint Security for Linux

1. In the main window of the Web Console, select **Software management** → **Installation packages**.
2. Click **Add**.

   The Wizard for creating an installation package will start.

3. Select **Create an installation package for a Kaspersky application**.

4. In the list of applications, find the latest version of Kaspersky Endpoint Security for Linux and click its name.

5. In the sidebar, begin the download by clicking the **Download and create installation package** button.

   Review and accept the End User License Agreements to start using the applications.

6. Go back to the list of applications and download the latest version of Network Agent for Linux.

   Review and accept the End User License Agreements to start using the applications.

7. In the main window of the Web Console, in the list of downloaded applications, click the names of the applications.

In an isolated network, download the distribution packages from the Kaspersky website and select the **Create an installation package from a file** option in the New package wizard.

Video: automatic creation of an installation package in Kaspersky Security Center

Video: manually creating an installation package in Kaspersky Security Center

8. Installing Network Agent for Linux

1. In the Web Console main window, select **Software management** → **Installation packages**.

2. Select the check box next to the **Kaspersky Network Agent for Linux** package.

3. Click **Expand**.

   The Protection Deployment Wizard starts.

4. Select the **Using a stand-alone package** option.

5. At the **Move devices to the Managed devices folder** step, skip the configuration of rules for moving devices to an administration group. This option is not applicable to the Administration Server device.

6. At the **Result of stand-alone installation package creation** step, select and copy the full path to the application installation script.

7. In the operating system of the Administration Server, open the command line.

8. Start the installation of the standalone package:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   where `</var/opt/.../stand-alone_package_sh>` is the previously copied full path to the standalone installation package script file of the application.

   If the installation is successful, a corresponding notification is displayed.

9. Move the Administration Server device (for example, *ksclinux*) from the **Managed devices** group to a previously prepared administration group (for example, *kscserver*).

9. Installing Kaspersky Endpoint Security for Linux

1. In the Web Console main window, select **Software management** → **Installation packages**.

2. Select the check box next to the Kaspersky Endpoint Security for Linux package.

3. Click **Expand**.

   The Protection Deployment Wizard starts.

4. Select the **Using a stand-alone package** option.

5. At the **Result of stand-alone installation package creation** step, select and copy the full path to the application installation script.

6. In the operating system of the Administration Server, open the command line.

7. Start the installation of the standalone package:

   ```
   sudo bash "</var/opt/.../stand-alone_package_sh>"
   ```

   where `</var/opt/.../stand-alone_package_sh>` is the previously copied full path to the standalone installation package script file of the application.

   If the installation is successful, a corresponding notification is displayed.

8. In the main window of the Web Console, in the **Tasks** section, select the root node in the list of administration groups with the name of the Administration Server.

9. From the list of Administration Server tasks, start the following tasks in sequence:
   - Download updates to the Administration Server repository
   - Update (Kaspersky Endpoint Security for Linux)
10. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.
11. Click the name of the Administration Server device object.
12. Check the main indicators of the device status:
   - The last update of the anti-virus databases (currently).
   - Connected to the Administration Server (currently).
   - Protection status (Running).
   - *Key added successfully* event (present).

Use the Kaspersky Endpoint Security for Linux deployment guide to deploy the security solution on devices in your network.

Updating the application from a previous version

The Kaspersky Endpoint Security application can be upgraded by remotely or locally installing a new version of the application on protected devices.

You can only upgrade to Kaspersky Endpoint Security 12.5 for Linux from Kaspersky Endpoint Security 12.4 for Linux.

Upgrading earlier Kaspersky Endpoint Security versions to version 12.5 is not supported. If you have an earlier version of Kaspersky Endpoint Security installed, you need to first uninstall it and then install Kaspersky Endpoint Security 12.5 for Linux.

You can follow these steps to upgrade the application.

1 Preparing the environment

Before starting the upgrade of Kaspersky Endpoint Security, complete the necessary preparatory steps depending on your infrastructure.

2 Preparing distribution packages

Select a distribution package depending on your operating system, its architecture and CPU type.

3 Updating the Kaspersky Endpoint Security management plug-in

If you are managing Kaspersky Endpoint Security using Kaspersky Security Center, update the Kaspersky Endpoint Security management web plug-in or MMC plug-in, depending on the console that you are using to manage Kaspersky Security Center.

4 Updating the application and graphical interface on protected devices

Install the new version of the application on your protected devices. The updated application retains the application usage mode that was selected during installation. If you want to use the application in a different mode, you must uninstall the application and then perform the installation and initial configuration of the application.

If you are using Kaspersky Endpoint Security in Basic mode or in EDR Agent mode and you use the graphical interface of the application, also update the graphical interface.

You can update the application and the application's graphical interface in the following ways:

- Remotely using Kaspersky Security Center
- Locally from the command line

How to upgrade the application from an RPM package using the command line

Upgrading the application on the command line amounts to installing a new version of the application on the device.

> You need root privileges to update the application.

To upgrade the application, run the following command:

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] rpm -U --replacefiles --
replacepkgs kesl-12.5.0-<build number>.<arch>.rpm [kesl-gui-12.5.0-<build number>.<arch>.rpm]
```

Kaspersky Endpoint Security will restart automatically.

Symbols

Command options

Setting	Description
`KESL_EULA_AGREED=yes`	Accept the terms and conditions of the End User License Agreement.
`KESL_PRIVACY_POLICY_AGREED=yes`	Accept the terms and conditions of the Privacy Policy.
`KESL_USE_KSN=yes/no`	Using Kaspersky Security Network: `yes` – accept the terms of the Kaspersky Security Network Statement and enable the use of Kaspersky Security Network. `no` – decline the terms of the Kaspersky Security Network Statement and disable the use of Kaspersky Security Network.

Setting	Description
`<arch>`	Architecture type: `i386` – for 32-bit operating systems `x86_64` – for 64-bit operating systems `aarch64` – for 64-bit operating systems for the Arm architecture

Kaspersky Endpoint Security will restart automatically.

Example:

```
Update the RPM application package with the GUI package for 64-bit operating systems:

# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes rpm -U --replacefiles --replacepkgs kesl-12.5.0-<build number>.x86_64.rpm kesl-gui-12.5.0-<build number>.x86_64.rpm
```

Changes to the application settings made after the update is complete and before the application restarts are not saved.

How to upgrade the application from a DEB package using the command line

Upgrading the application on the command line amounts to installing a new version of the application on the device.

You need root privileges to update the application.

To upgrade the application, run the following command:

```
# [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=<yes|no>] apt-get install ./kesl_12.5.0-<build number>_<arch>.deb [./kesl-gui_12.5.0-<build number>_<arch>.deb]
```

Kaspersky Endpoint Security will restart automatically.

Symbols

Command options

Setting	Description
`KESL_EULA_AGREED=yes`	Accept the terms and conditions of the End User License Agreement.
`KESL_PRIVACY_POLICY_AGREED=yes`	Accept the terms and conditions of the Privacy Policy.
`KESL_USE_KSN=yes/no`	Using Kaspersky Security Network: `yes` – accept the terms of the Kaspersky Security Network Statement and enable the use of Kaspersky Security Network. `no` – decline the terms of the Kaspersky Security Network Statement and disable the use of Kaspersky Security Network.
`<arch>`	Architecture type: `i386` – for 32-bit operating systems `amd64` – for 64-bit operating systems `arm64` – for 64-bit operating systems for the Arm architecture

Example:

```
Update the DEB application package with the GUI package for 64-bit operating systems:

# KESL_EULA_AGREED=yes KESL_PRIVACY_POLICY_AGREED=yes KESL_USE_KSN=yes apt-get install ./kesl_12.5.0-<build number>_amd64.deb [./kesl-gui_12.5.0-<build number>_amd64.deb]
```

Changes to the application settings made after the update is complete and before the application restarts are not saved.

5 Updating the Kaspersky Security Center Network Agent

Optional step. If you are centrally managing Kaspersky Endpoint Security using Kaspersky Security Center, update the Network Agent on the protected devices. The upgrade is performed by installing a new version of Network Agent.

On a device running the Astra Linux Special Edition operating system, we recommend to update Network Agent remotely using Kaspersky Security Center, since updating using the command line in the Kaspersky Security Center administration console creates a new copy of the same managed device, and the old one becomes inaccessible. For more details, see the Kaspersky Security Center Help.

The application continues working correctly during the Network Agent update.

Features of upgrading a previous version of the application

- If an error occurs while updating the application, the update is rolled back and the previous version of the application is started. In this case, an error message will be displayed, but the package manager (rpm/dpkg) will indicate the new version.

- On an operating system with a package manager of the `rpm` type, if the application package and the GUI package are both installed, we do not recommend updating only one of the packages without the other.

  On an operating system with a package manager of the `dpkg` type, if the application package and the GUI package are both installed, either of the packages cannot be updated without the other.

- If the terms and conditions of the End User License Agreement and/or the Privacy Policy have changed in the new version of the application, you must accept the new terms and conditions during the update. Texts of user agreements are available at the Kaspersky website (in the **EULA** section), as well as in the `~/.kesl/12.5/license.<language ID>` directory.

  If you do not accept the conditions of the End User License Agreement and/or the Privacy Policy, the application will not be updated.

- If the terms of the Kaspersky Security Network Statement changed in the new version of the application, you need to accept or decline the new terms of use for participating in Kaspersky Security Network. You can find the text of the Kaspersky Security Network Statement is available in the ~/.kesl/12.5/ksn_license.<language ID>. Refusal to use Kaspersky Security Network does not interrupt the update process. You can enable, disable, or change Kaspersky Security Network mode later.

  If you used KSN and accepted the conditions of the Kaspersky Security Network Statement in a previous version of the application, you need to accept the conditions of the Kaspersky Security Network Statement when updating the application. Otherwise, use of KSN will be disabled.

- Even if Kaspersky Endpoint Security is launched before the update process start, if the update is completed successfully, a new application version is launched.

- When you update the application to a newer version, the dump files of the previous version are deleted.

- When you update the application, the event log file from the previous version becomes the first event file in the set of files of the current version. This file is kept until the number of events in the remaining files reaches the specified maximum number (the `MaxEventsNumber` setting). Therefore, a transient situation is possible wherein the application stores twice as many events as specified in the `MaxEventsNumber` setting.

- If Kaspersky Endpoint Security is being used in Basic mode or in the EDR Agent mode, we recommend starting the database update task after updating the application.

Updating Kaspersky Endpoint Security management plug-ins

The administration plug-in for Kaspersky Endpoint Security is updated by installing the new version of the administration plug-in. Depending on the Kaspersky Security Center administration console that you use, you have to install:

- Kaspersky Endpoint Security management web plug-in

- Kaspersky Endpoint Security MMC management plug-in

How to install the management web plug-in

You can install the web plug-in:

- Using the Quick Start Wizard for Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console automatically prompts you to run the Quick Start Wizard when connecting Kaspersky Security Center Web Console to the Administration Server for the first time. You can also run the Initial Configuration Wizard in the Kaspersky Security Center Web Console interface (**Device discovery and deployment** → **Deployment and assignment** → **Quick Start Wizard**). The Quick Start Wizard can also check if the installed web plug-ins are up to date and download the necessary updates. For details on the Quick Start Wizard for Kaspersky Security Center Web Console, refer to the Kaspersky Security Center Help.

- Manually, using a distribution kit from the list of Kaspersky Web plug-ins or from a file.

To install the Kaspersky Endpoint Security web plug-in manually from Kaspersky Security Center:

1. In the main window of the Kaspersky Security Center Web Console, select **Settings** → **Web plug-ins**.

   A list of installed web plug-ins opens.

2. Click the **Add** button.

   This opens the list of available management plug-ins. The list is updated automatically after new versions of web plug-ins are released.

3. In the list of available plug-ins, select the **Kaspersky Endpoint Security <version number> for Linux** web plug-in.

4. In the window that opens with a description of the web plug-in, click the **Install plug-in** button.

5. Wait for the installation to complete and click **OK** in the information window.

The new plug-in will be displayed in the list of installed web plug-ins (**Settings** → **Web plug-ins**).

To install the Kaspersky Endpoint Security web plug-in manually from a file:

1. Download the archive with the Web Plug-in from the application download page in the **Kaspersky Endpoint Security for Linux** section (**Additional distribution package** → **Web console Plug-in**).

2. Unpack the downloaded archive locally.

3. In the main window of the Kaspersky Security Center Web Console, select **Settings** → **Web plug-ins**.

   A list of installed web plug-ins opens.

4. Click the **Add from file** button.

5. This opens a window; in that window, specify the path to the plugin.zip file and the path to the signature.txt file. The files are located in the folder to which you unpacked the archive with the Web Plug-in.

6. Click the **Add** button.

7. Wait for the installation to complete and click **OK** in the information window.

The new plug-in is displayed in the list of installed web plug-ins (**Settings** → **Web Plug-ins**).

If you select a language that is not included in Kaspersky Endpoint Security distribution package in the properties of Kaspersky Security Center Administration Server, the License Agreement and the entire Kaspersky Security Center Web Console interface will be displayed in English.

How to install the MMC management plug-in

Before installing Kaspersky Endpoint Security MMC management plug-in, make sure that Kaspersky Security Center and Redist C++ 2015 (Microsoft Visual C++ 2015 Redistributable) are installed.

To install the MMC plug-in:

1. Download the klcfginst.msi file on the application download page in the **Kaspersky Endpoint Security for Linux** section (**Build** → **Administration Plug-In**).

2. On the device where the Kaspersky Security Center Administration Console is installed, run the klcfginst.msi file.

After installation, the MMC management plug-in is displayed in the list of installed MMC management plug-ins in the properties of the Kaspersky Security Center Administration Server.

To view the list of installed management MMC plug-ins:

1. In the Kaspersky Security Center Administration Console tree, select the **Administration Server <server name>** node and open the Administration Server properties window in one of the following ways:
   - Open the context menu of the **Administration Server <server name>** node and select the **Properties** item.
   - Click the **Administration Server properties** link in the workspace of the **Administration Server <server name>** node in the **Administration Server** section.
2. In the list on the left, in the **Advanced** section, select the **Information about the installed application management plug-ins** section.

   In the right part of the window, the list of installed administration plug-ins displays the administration MMC plug-in for Kaspersky Endpoint Security: **Kaspersky Endpoint Security <version number> for Linux**.

Converting policies and tasks

Policies and tasks configured for previous versions of Kaspersky Endpoint Security are not compatible with the updated version of the application. If you use the Kaspersky Security Center Administration Console to manage the application, then after updating the MMC management plug-in, you can convert policies and tasks using the Kaspersky Security Center Policies and Tasks Batch Conversion Wizard (for details, see the Kaspersky Security Center Help).

Converted policies and tasks are named "*<Name of the original policy or task> (converted)*".

For most settings, converted policies and tasks use the values configured for the previous version of the application. Some settings are assigned special values. The settings that were not configured in the policies and tasks of the previous version take default values in the converted policies and tasks.

> You cannot convert policies and tasks in the Kaspersky Security Center Web Console.

If you use the Web Console to manage the application, you must create new policies and tasks for the application in Kaspersky Security Center. You can migrate some values of settings of policies and tasks from a previous version of a policy or task to a new one by exporting and importing settings.

Special considerations of management plug-ins

- Management plug-ins of the previous version continue to work after installing the new version of Kaspersky Endpoint Security management plug-ins. You can use them to manage the previous version of Kaspersky Endpoint Security.

  If you have updated the application on all client devices, you can uninstall the Kaspersky Endpoint Security administration plug-ins of the previous version.

- When installing a new build of the MMC management plug-in for the same version of the application, you must first uninstall the currently installed MMC plug-in of this version, and then install the new MMC plug-in of this version.

Application settings after upgrade

If you use Kaspersky Security Center Administration Console to manage the application, you can *convert policies* to have the new version use the values of policy settings specified for the previous version of the application (for more information, see the Kaspersky Security Center Help).

> You cannot convert policies in the Kaspersky Security Center Web Console.

After updating the application using the command line, most settings carry over from the previous version of the application. You can also migrate application settings by exporting settings to a file and then importing them from that file.

Default values are assigned to settings that did not exist in the previous version of the application. Some settings are assigned special values.

System event interception settings

If the system event interception mechanism based on the updatable kernel module was selected in the previous version of the application, after the update, the application switches to intercepting system events using the fanotify. Then, after updating the databases and application modules and automatically restarting, the application reverts to using the updatable kernel module again.

Kaspersky Security Network settings

After converting a policy in the MMC plug-in, the Kaspersky Security Network settings in the policy properties depend on whether you accepted or rejected the terms of the Kaspersky Security Network Statement in the Policies and Tasks Batch Conversion Wizard:

- If you accepted the terms of the Statement, the **Extended KSN mode** option is selected.

- If you rejected the terms of the Statement, the **Do not use KSN** option is selected.

After updating the application on the command line, the `UseKSN` setting is modified as follows:

- If you set `KESL_USE_KSN=No` during upgrade, `UseKSN=No`.
- If you set `KESL_USE_KSN=Yes` during upgrade, `UseKSN=Extended`.
- In other cases, the value of the `UseKSN` setting does not change after the update.

Cloud mode settings

After converting a policy in the MMC plug-in, the settings for using cloud mode may change depending on whether you accepted or rejected the terms of the Kaspersky Security Network Statement in the Policies and Tasks Batch Conversion Wizard:

- If you accepted the terms of the Statement, the **Enable cloud mode** check box will be selected.
- If you rejected the terms of the Statement, the **Enable cloud mode** check box will be cleared.

After updating the application on the command line, `CloudMode` is set to:

- `CloudMode=No` if `UseKSN=No` after the upgrade.
- `CloudMode=Yes` if `UseKSN=Basic/Extended` was set after the update and `CloudMode=Yes` was set before the update.

Cloud mode is available if use of KSN is enabled. To enable cloud mode:

- in the Administration Console or in the Web Console, select the **Extended KSN mode** option and select the **Enable cloud mode** check box.
- On the command line, set the following settings:

```
UseKSN=<Basic|Extended>
CloudMode=Yes
```

Kaspersky Managed Detection and Response integration settings

If the MDR component was enabled, after converting the policy in the MMC plug-in, the status of the MDR component depends on whether you have accepted or rejected the terms of the Kaspersky Security Network Statement in the Policies and Tasks Conversion Wizard:

- If you have accepted the terms of the Statement, the MDR component remains enabled (the **Enable Managed Detection and Response** check box is selected).
- If you have rejected the terms of the Statement, the **Enable Managed Detection and Response** check box is cleared.

After updating the application on the command line, `UseMDR` is set to:

- `UseMDR=No` if `UseKSN=No` after the upgrade.
- `UseMDR=Yes` if `UseKSN=Basic/Extended` was set after the update and `UseMDR=Yes` was set before the update.

If you want to use the Kaspersky Managed Detection and Response functionality, you need to enable the extended mode of Kaspersky Security Network.

Endpoint Detection and Response Expert integration settings

The new version of the application provides a Kaspersky Endpoint Detection and Response Expert (cloud) integration mode.

Integration of Kaspersky Endpoint Security for Linux with Kaspersky Endpoint Detection and Response Expert (cloud) is temporarily unavailable. This functionality is planned to be supported by the end of 2026. Keep track of our Release Notes to be aware of application upgrades and new features.

After converting the policy in the MMC plug-in, integration with Endpoint Detection and Response Expert (cloud) is disabled (the **Enable Endpoint Detection and Response Expert (cloud)** check box is cleared). The application uses the Endpoint Detection and Response Expert (on-premises) integration.

After updating the application on the command line, `EDR_EXPERT_CLOUD_MODE` is set to: `EDR_EXPERT_CLOUD_MODE=No` (default value).

User permission settings

The new version of the application supports Password protection.

After converting the policy in the MMC plug-in, Password protection is disabled.

After upgrading the application using the command line, user permissions are preserved in accordance with the user roles (*kesladmin*, *kesluser*, *keslaudit*, *nokesl*) configured in the previous version of the application.

Uninstalling the application

You can follow these steps to uninstall Kaspersky Endpoint Security.

Special considerations for removing Kaspersky Endpoint Security for Linux

- While the application is being uninstalled, all Kaspersky Endpoint Security tasks will be stopped on the device.
- After uninstalling the application, all information saved by the application is deleted, including any application certificates that were installed. The license database is saved, and you can use it to reinstall the application. The unique computer ID (SensorID) is also saved.
- If the application was installed in a systemd, the systemd settings are restored to their initial state after the application uninstallation.

1 Uninstalling the application and graphical interface of the application

Uninstall the application packages and graphical interface packages from the protected devices.

You can uninstall both the application package and the graphical interface package, or uninstall only the graphical interface package. It is not possible to uninstall only the application package if the graphical interface package is installed.

You can uninstall the application and the application's graphical interface in the following ways:

Remotely using Kaspersky Security Center

Locally from the command line

> Uninstallation requires root privileges.

After the uninstallation procedure is complete, a message about the results of the uninstallation is displayed.

Removing the application package and the graphical user interface package

```
Uninstall the application and the graphical interface installed from RPM packages
rpm -e kesl kesl-gui
```

```
Uninstall the application and the graphical user interface installed from DEB packages
apt-get purge kesl kesl-gui
```

Removing the application package that was used without a graphical interface

```
Delete the application installed from an RPM package
rpm -e kesl
```

```
Delete the application installed from a DEB package
apt-get purge kesl
```

Removing the graphical user interface package

```
Uninstall the graphical interface of the application installed from an RPM package
rpm -e kesl-gui
```

```
Uninstall the graphical interface of the application installed from a DEB package
apt-get purge kesl-gui
```

Uninstallation is performed in the background.

2 Removing Network Agent

If you were using Kaspersky Security Center to manage Kaspersky Endpoint Security, you must uninstall the Network Agent from protected devices.

You can uninstall Network Agent in the following ways:

Remotely using Kaspersky Security Center

Locally from the command line

Uninstallation requires root privileges.

After the uninstallation procedure is complete, a message about the results of the uninstallation is displayed.

```
Uninstall the Network Agent installed on a 32-bit operating system from an RPM package
rpm -e klnagent
```

```
Uninstall the Network Agent installed on a 64-bit operating system from an RPM package
rpm -e klnagent64
```

```
Uninstall the Network Agent installed on a 32-bit operating system from a DEB package
apt-get purge klnagent
```

```
Uninstall the Network Agent installed on a 64-bit operating system from a DEB package
apt-get purge klnagent64
```

3 Uninstalling the Kaspersky Endpoint Security management plug-in

If you were using Kaspersky Security Center to manage Kaspersky Endpoint Security, you must uninstall the Kaspersky Endpoint Security administration web plug-in or MMC plug-in, depending on the console that you were using to manage Kaspersky Security Center.

How to remove the Kaspersky Endpoint Security MMC management plug-in

1. Close the Kaspersky Security Center Administration Console.

2. On the device where the Kaspersky Security Center Administration Console is installed, open the Windows registry editor and go to:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins
   ```

   This key contains information about all management plug-ins installed in the Administration Console. The name of the managed application is in the **DisplayName** value.

3. Select the section corresponding to the relevant version of the Kaspersky Endpoint Security application plug-in.

4. Open and copy the **UninstallString** value.

5. Open the command prompt as administrator, paste the copied value and press **`Enter`**.

How to remove the Kaspersky Endpoint Security management web plug-in

1. In the main window of the Kaspersky Security Center Web Console, select **Settings** → **Web plug-ins**.

   A list of installed web plug-ins opens.

2. Select the **Kaspersky Endpoint Security <version number> for Linux** check box.

3. Click **Delete**.

   Confirm the uninstallation of the web plug-in.

Using the application

By default, Kaspersky Endpoint Security starts automatically when the operating system is booted (at the default level of execution for each operating system).

When the application is launched with the default configuration, the following components are started:

- File Threat Protection.
- Device Control.
- Behavior Detection.
- Web Threat Protection—only if one of the supported browsers is installed in the operating system and local management of Web Threat Protection settings is allowed on the device (a policy is not applied or the "lock" is not set in the policy properties).
- Network Threat Protection—only if the Network Threat Protection settings on the device are defined through a policy. Network Threat Protection is enabled in the policy properties by default. If locally configured settings are applied on the device, Network Threat Protection is disabled by default.

When the application is started, service tasks are automatically started on the device to ensure the operation of additional application functions: the application activation function and the Backup function.

By default, the application also starts user tasks configured on the command line, for which the "after application startup" run mode (PS run mode) is configured.

If you stop the application, all tasks running on the device will be interrupted. Interrupted user tasks with the PS run mode are not resumed from where they left off. The next time the application is launched, such a task will be executed from the beginning rather than resumed from where it was interrupted. For more information about task types, see the Kaspersky Endpoint Security Local Tasks section.

The Kaspersky Endpoint Security status is monitored by the watchdog service. The watchdog service is automatically launched when the application starts. In the event of an application crash, a dump file is generated and the application is restarted automatically.

How to start or stop the application using the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. In the list, select the device on which you want to start or stop the application, and click the link with the device name to open the device properties window.

3. Select the **Applications** tab.

4. Select the Kaspersky Endpoint Security check box.

5. Do one of the following:

   - To start the application, click the **Start** button.
   - To stop the application, click the **Stop** button.

You can monitor the application operation status by using the **Protection status** widget in the **Monitoring and reports / Dashboard** window.

How to start or stop the application using the Administration Console

1. In the Administration Console tree, in the **Managed devices** folder, select the administration group containing the necessary device.
2. In the workspace, select the **Devices** tab.
3. In the list of managed devices, select the device for which you want to start or stop the application. In the device context menu, select **Properties**.
4. In the **Properties: <Device name>** window, select the **Applications** section.

   The right part of the window displays a list of Kaspersky applications installed on the device.
5. Select Kaspersky Endpoint Security.
6. Do one of the following:

   – start the application.

   – stop the application.

   You can also manage the application from the context menu.

How to start or stop the application using the command line

To run the application, the root account must be the owner of the following directories and only the owner must have write access to them: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Operating system with systemd

Start the application

```
systemctl start kesl
```

Stop the application

```
systemctl stop kesl
```

Restart the application

```
systemctl restart kesl
```

Display the current status of the application

```
systemctl status kesl
```

Operating system with init

```
Start the application
service kesl start
```

```
Stop the application
service kesl stop
```

```
Restart the application
service kesl restart
```

```
Display the current status of the application
service kesl status
```

Licensing

A *license* is a time-limited right to use Kaspersky Endpoint Security, granted under the End User License Agreement. The list of available functions and the validity period of the application depend on the license under which the application is used.

License types

Free

- *Trial* – a free license intended for trying out the application.

  Trial licenses have a short validity period. When the trial license expires, all Kaspersky Endpoint Security features become disabled. To continue using the application, you need to purchase a commercial license.

  You can activate the application under a trial license only once. After the application has been activated under a commercial license, it can no longer be activated under a trial license.

- The *Kaspersky Security Center Cloud Console trial license* is a license intended for evaluating the Cloud Console. With this license, you can perform actions in a workspace for a period of 30 days. All managed applications, including Kaspersky Endpoint Security, are automatically activated under Kaspersky Security Center Cloud Console trial license. However, you cannot activate Kaspersky Endpoint Security using its own trial license when the trial license for the Cloud Console expires.

  The trial workspace will be automatically deleted with all its contents after the 30-day period expires.

Paid

- *Commercial* – a paid license that is provided when you purchase the application.

  The main functions of the application stop working when a commercial license expires. To continue using Kaspersky Endpoint Security, you need to renew the commercial license. After the license expires, you can no longer use the application and must uninstall it from the device.

- *Subscription* is a purchase order for the application with specific parameters (subscription expiration date, number of protected devices). You can purchase a subscription from a service provider in your region.

Subscription can be limited (for one year, for example) or unlimited (without an expiry date). When a limited subscription expires, you may be provided a subscription renewal grace period during which the application continues to function. The service provider decides whether or not to grant a grace period and, if so, determines the duration of the grace period.

You can manage your subscription, including canceling it, on the website of the service provider.

How licensing works

1. **You will receive an activation code**

   After you have purchased a Kaspersky solution on the official Kaspersky website or from one of our partners, you will receive a message at the email address that you specified during the purchase. This message will contain an activation code and information on how to get a key file. You may need a key file if your organization does not support online activation of the application using a code.

   > If you have purchased a subscription to Kaspersky Endpoint Security, the service provider will only provide you with an activation code.

2. **Activating the application**

   Next, you need *activate the application*, that is, make an application license current. To do this, you need to add a license key to the application using your activation code or key file.

   The following activation methods are provided:

   - Remotely, using Kaspersky Security Center
   - On the command line
   - Via the graphical interface

   Standard mode

   To use the application in standard mode, you can use licenses that cover different scopes of functionality. If some components are not covered by your license, you may need another license key:

   - Kaspersky Endpoint Detection and Response Optimum Add-on license key (hereinafter also referred to as the *EDR Optimum key*), for activating the Kaspersky EDR Optimum component
   - Kaspersky Unified Monitoring and Analysis Platform Add-on license key (hereinafter also referred to as the *KUMA key*), for activating integration with the Kaspersky Unified Monitoring and Analysis Platform functionality
   - Kaspersky Managed Detection and Response Optimum/Expert Add-on license key (hereinafter also referred to as the *MDR key*), for activating the Kaspersky MDR component
   - Kaspersky Endpoint Detection and Response Expert (on-premises) Add-on license key (hereinafter also referred to as the *EDR Expert (on-premises) key*), for activating the EDR Expert (on-premises) component
   - Kaspersky Endpoint Detection and Response Expert (cloud) Add-on license key (hereinafter also referred to as the *EDR Expert (cloud) key*), for activating the EDR Expert (cloud) component
   - Kaspersky Workload Security Module Add-on license key (hereinafter also referred to as the *KWSM key*), for activating the System Integrity Monitoring and Container Scan components

If these components are not covered by your license, you can activate them only after activating the Kaspersky Endpoint Security application itself.

EDR Agent mode

If you are using the Kaspersky Endpoint Security application in EDR agent mode, you need an EDR Expert (on-premises) license key to activate it.

Light Agent mode

If you are using Kaspersky Endpoint Security in Light Agent mode, you do not need to add a key to the application. You activate Kaspersky Security for Virtualization Light Agent on the Protection Server side.

The Endpoint Detection and Response Optimum component and components for integration with Kaspersky solutions are also activated on the Protection Server side.

Troubleshooting application activation issues

3. **Renewing a license or subscription**

   We recommend keeping an eye on your license or subscription to renew it in a timely manner. We recommend renewing the license before its expiration date to ensure continued protection of your device against security threats.

   For timely renewal of the license, you can use a reserve key. You can renew your subscription manually or automatically on the website of your service provider. Unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

   Special considerations involved in adding keys

   - A trial license key or a subscription key cannot be added as a reserve key.
   - The expiration date of the reserve key must be later than the expiration date of the active key.
   - If an active key as well as a reserve key have been added to the application, and you add a new active key, the new key replaces the previously added active key; if you add a new reserve key, it replaces the previously added reserve key.
   - If an active key and keys for activating the Endpoint Detection and Response Optimum component and components for integration with Kaspersky solutions have been added to the application, and you have added one reserve key for a license that also covers the Endpoint Detection and Response Optimum component and components for integration, then after the active key expires, the reserve key becomes active and releases the other active keys. You can then use these keys to activate the Endpoint Detection and Response Optimum component and the integration components on another device.

4. **Viewing information about added license keys**

   You can view information about license keys added to the application remotely using Kaspersky Security Center or using the command line or graphical interface locally on a protected device.

Useful articles

End User License Agreement

The *End User License Agreement* 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 read the End User License Agreement and the Privacy Policy, which describes data processing and provision:

- Before installing the application in the license.<language identifier> file. This file is included in the application distribution kit.
- During Kaspersky Endpoint Security installation.

  By confirming your consent to the terms and conditions of the End User License Agreement and the Privacy Policy when creating the application installation package (if installed using Kaspersky Security Center) or during the initial application configuration (if installing using the command line), you accept the terms and conditions of the End User License Agreement and the Privacy Policy. If you do not accept the terms of the End User License Agreement or Privacy Policy, you must cancel the installation of the application and may not use the application.

- After the application is installed, the files containing the texts of the End User License Agreement of the Kaspersky application and the Privacy Policy are located on the protected device in the /opt/kaspersky/kesl/doc/license.<language ID> directory.

Activation code

An *activation code* is a unique sequence of 20 alphanumeric characters.

To activate the application with an activation code, you need Internet access in order to connect to Kaspersky activation servers.

If you lost your activation code after activating the application, contact the Kaspersky partner from whom you purchased the license.

Key file

A *key file* is a file with the .key extension that you receive from Kaspersky. To activate the application with a key file, you do not need to connect to Kaspersky activation servers.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, perform any of the following actions:

- Contact the license seller.
- Obtain a key file on the Kaspersky website based on your existing activation code.

License key

A *license key* is a sequence of bits that you can use to activate and then use the application in accordance with the terms of the End User License Agreement. License key is generated by Kaspersky experts.

The key that the application is currently activated with becomes the *active license key*. As the active key, you can add a trial license key, commercial license key (commercial key), or subscription key.

Reserve key

Reserve license key is a license key that entitles the user to use the application, but is not currently in use. The reserve license key automatically becomes active when the license associated with the current active license key expires. A reserve key can be added only after an active key has been added.

A trial license key can only be added as an active license key. A license key for a trial license cannot be added as a reserve license key.

How to switch to another Kaspersky solution

> If the application is used in Light Agent mode, license keys are managed in the Kaspersky Security for Virtualization Light Agent solution.

Follow these steps if your organization has a Kaspersky solution deployed, Kaspersky Endpoint Security is used in Standard mode or EDR Agent mode, and you need to switch to another Kaspersky solution.

1. **Prepare a new license**

   Purchase another Kaspersky solution on the Kaspersky website or from our partners. You will receive an email message at the email address that you specified during the purchase. This message will contain an activation code and information on how to get a key file.

   If you have previously activated the Kaspersky Endpoint Security application using an activation code, this time you will also need to use an activation code. If you have previously activated the application using a key file, you will need to use a key file.

2. **Replace your license**

   You can replace a license in the following ways:

   - Remotely using Kaspersky Security Center. Add the license key to the Administration Server repository and distribute it to protected devices.
   - On the command line using the following command: `kesl-control [-L] --add-active-key <path to key file / activation code>`.
   - In the graphical interface, delete the key that is currently applied to the application and add the new key.

3. **Make sure the license has been replaced successfully**

   To do so, view the details of the license key that is used on your protected devices.

Useful articles

Activation code

An *activation code* is a unique sequence of 20 alphanumeric characters.

To activate the application with an activation code, you need Internet access in order to connect to Kaspersky activation servers.

If you lost your activation code after activating the application, contact the Kaspersky partner from whom you purchased the license.

Key file

A *key file* is a file with the .key extension that you receive from Kaspersky. To activate the application with a key file, you do not need to connect to Kaspersky activation servers.

You can restore a key file if it has been accidentally deleted. You may need a key file to register a Kaspersky CompanyAccount, for example.

To restore your key file, perform any of the following actions:

- Contact the license seller.
- Obtain a key file on the Kaspersky website based on your existing activation code.

Managing license keys

> If the application is used in Light Agent mode, license keys are managed in the Kaspersky Security for Virtualization Light Agent solution. License key management commands return an error.

Key management using Kaspersky Security Center

In Kaspersky Security Center, you can add keys to managed devices in the following ways:

- Using the *Add key* task. This method allows adding keys to the application on an individual device or on all devices included in an administration group. When creating a task, it uses the key that is added to the Kaspersky Security Center key store. You can add a license key to the key store in advance or when creating the Add key task.
- By distributing a key stored on the Kaspersky Security Center Administration Server to the devices. This method lets you automatically add keys to the managed devices that are already connected to Kaspersky Security Center, and to new managed devices. To use this method, first add the key to the Kaspersky Security Center key store.

  During the automatic distribution of a key as an active or a reserve key, the licensing limit on the number of devices (set in the key properties) is taken into account. If the licensing limit is reached, distribution of this key to the devices stops automatically. You can view the number of devices to which the key has been added and other information in the key properties on the **Devices** tab.

How to add a key to Kaspersky Security Center key storage using the Web Console

1. In the Web Console main window, select **Operations** → **Kaspersky Licenses**.
2. Click the **Add** button.
3. In the window that opens, select how to add the key to the repository:
   - **Enter the activation code** to add a key using an activation code.
   - **Add a key file** to add a key using a key file.

4. Depending on the key adding method you selected at the previous step, do one of the following:
   - Enter the activation code and click **Submit**.
   - Click the **Select key file** button and in the window that opens, select a file with the .key extension.
5. Click the **Close** button.

The added key will appear in the list of keys.

How to add a key to the application via the Web Console using an Add Key task

1. In the main window of the Web Console, select **Tasks**.
   The list of tasks opens.
2. Click the **Add** button.
   The Task Wizard starts.
3. Configure the task settings:
   a. In the **Application** drop-down list, select the application name: Kaspersky Endpoint Security.
   b. In the **Task type** drop-down list, select **Add Key**.
   c. In the **Task name** field, enter a brief description, such as *Activation of Kaspersky Endpoint Security*.
   d. In the **Devices to which the task will be assigned** section, select the task scope. Click **Next**.
4. Select devices according to the selected task scope option. Click **Next**.
   This opens the **Select the license** window.
5. If you have previously added a key to Kaspersky Security Center key storage, select the key from in the list and click **Next**.
6. If the key that you need is not present in the key store, click the **add a new license key** link.
   a. In the window that opens, select how to add the key to the repository:
      - **Enter the activation code** to add a key using an activation code.
      - **Add a key file** to add a key using a key file.
   b. Depending on the key adding method you selected at the previous step, do one of the following:
      - Enter the activation code and click **Submit**.
      - Click the **Select key file** button and in the window that opens, select a file with the .key extension.
   c. Read the information about the key and click **Close**.
   d. The added key will appear in the list of keys. Select it from the list and click **Next**.
7. Read the information about the license and click **Next**.

8. On the **Application settings** tab, you can select the **Use as a reserve key** check box. A key added as a reserve key becomes active after the current key expires.

9. Finish the wizard.

   A new task will be displayed in the list of tasks.

10. Select the check box next to the task. Click the **Start** button.

How to add a key to the application using the Web Console by distributing the key to devices

1. In the Web Console main window, select **Operations** → **Kaspersky Licenses**.

2. Open the key properties using the link with the name of the application for that the key is intended to.

3. On the **General** tab, select the **Automatically distribute a license key to managed devices** check box.

4. Click the **Save** button.

   The license key is automatically distributed to the appropriate client devices.

> A new license key is added to a device only if the application has not yet been activated on the device or if the license expires in less than 14 days.

Key management on the command line

To manage license keys on a device, you can use license key management commands.

How to add a key to the application

You can use these commands to add keys for activating the application keys for activating components that are not covered by your license. You do not need to specify the type of the key in the command.

```
Add an active license key to the application

kesl-control [-L] --add-active-key <path to key file / activation code>
```

Where:

- `path to key file` is the path to the key file. If the key file is located in the current directory, it is sufficient to specify only the file name.

- `activation code` is the activation code.

```
Add a reserve license key to the application

kesl-control [-L] --add-reserve-key <path to key file / activation code>
```

> If an active key has not yet been added to the application on the device, the command fails.

How to delete a key

Various commands are available for deleting keys.

Delete active key

```
kesl-control [-L] --remove-active-key
```

Delete reserve key

```
kesl-control [-L] --remove-reserve-key
```

Delete active EDR Optimum key

```
kesl-control [-L] --remove-active-key --edr-optimum
```

Delete reserve EDR Optimum key

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

Delete active KUMA key

```
kesl-control [-L] --remove-active-key --kuma
```

Delete reserve KUMA key

```
kesl-control [-L] --remove-reserve-key --kuma
```

Delete active MDR key

```
kesl-control [-L] --remove-active-key --mdr
```

Delete reserve MDR key

```
kesl-control [-L] --remove-reserve-key --mdr
```

Delete active EDR Expert (on-premises) license key

```
kesl-control [-L] --remove-active-key --edr-kata
```

Delete reserve EDR Expert (on-premises) license key

```
kesl-control [-L] --remove-reserve-key --edr-kata
```

Delete the active EDR Expert (cloud) key

```
kesl-control [-L] --remove-active-key --cxdr
```

Delete the reserve EDR Expert (cloud) key

```
kesl-control [-L] --remove-reserve-key --cxdr
```

Delete active KWSM key

```
kesl-control [-L] --remove-active-key --khcs
```

Delete reserve KWSM key

```
kesl-control [-L] --remove-reserve-key --khcs
```

Key management in the graphical interface

How to add an active license key

1. Open the main window of the application graphical interface.
2. Do one of the following:
   - In the lower part of the main window, click the area that displays information about the license and the key.
   - In the lower part of the main window, click the **Support** button to open the **Support** window, and in that window, click either the **License key** or the **Licenses** link in the lower part of the window.

   This opens the **Licenses** window.

   Clicking the **Purchase a license** button in this window opens the Kaspersky online store, where you can purchase a license.

3. If you want to activate the application under a commercial license:

   a. Click the **Add** button in the **Commercial key** section and perform the following actions, depending on the method you are using to add the key:

      - If you want to add a key using an activation code, enter the activation code and click the **Next** button.

      - If you want to add a key using a key file, click the **Select a key file** link to open the file selection window that window, select the file with the .key extension.

      This window displays information about the key and the license associated with it.

   b. Click the **Activate** button.

4. If you want to activate the application under a trial license, click the **Activate** button in the **Trial key** section. This window displays information about the trial license and the key associated with it.

How to add a reserve license key

1. Open the main window of the application graphical interface.

2. Do one of the following:

   - In the lower part of the main window, click the area that displays information about the license and the key.

   - In the lower part of the main window, click the **Support** button to open the **Support** window, and in that window, click either the **License key** or the **Licenses** link in the lower part of the window.

   This opens the **Licenses** window. The window displays information about previously added license keys.

3. Click the **Add** button and perform the following actions, depending on the method you are using to add the key:

   - If you want to add a key using an activation code, enter the activation code and click the **Next** button.

   - If you want to add a key using a key file, click the **Select a key file** link to open the file selection window that window, select the file with the .key extension.

   This window displays information about the key and the license associated with it.

4. Click the **Add** button.

How to remove a license key

1. Open the main window of the application graphical interface.

2. Do one of the following:

   - In the lower part of the main window, click the area that displays information about the license and the key.

   - In the lower part of the main window, click the **Support** button to open the **Support** window, and in that window, click either the **License key** or the **Licenses** link in the lower part of the window.

   This opens the **Licenses** window. The window displays information about previously added license keys.

3. Click the **Remove** button to the right of the information about the key that you want to remove.

4. Confirm the removal in the window that opens.

Useful articles

Troubleshooting application activation issues

Viewing information about license keys

Information about license keys in Kaspersky Security Center

You can view information about the license keys being used by Kaspersky Endpoint Security in the following ways:

- In the properties of the *Add key* task that you use to activate the application, you can find information about the key that this task adds to the application.

- In the properties of the Kaspersky application installed on the client device, you can find information about the active and reserve keys added to the application on this device.

  How to view information about license keys on a device using the Web Console

  1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

     The list of managed devices opens.

  2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

     The list displays only the managed devices for the selected administration group.

  3. Click the name of a device.

  4. This opens a managed device properties window; in that window, go to the **Applications** tab.

  5. In the list of applications installed on the device, click Kaspersky Endpoint Security.

  6. This opens the application properties window; in that window, go to the **Licenses** section on the **General** tab.

     This section displays information about license keys added to the application and the licenses associated with these keys.

     - **License key status** is the type of the key: active or reserve.

     - **Application name** is the name of the license associated with the key and information about this license.

     - **License key** is the license key, a unique alphanumeric sequence.

     - **License type** can be trial, commercial, or subscription.

- **Activation date** is the date when this key was added.
- **Expiration date** is the date when your right to use the application activated by adding this key expires.

How to view information about license keys on a device using the Administration Console

1. In the Kaspersky Security Center Administration Console tree, in the **Managed devices** folder, select the administration group containing the required device.
2. In the workspace, select the **Devices** tab.
3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.
4. In the displayed window with the properties of the managed device, select the **Applications** section.

   The right part of the window displays a list of Kaspersky applications installed on the device.
5. Select Kaspersky Endpoint Security and double-click it to open the application properties window. Alternatively, you can use the **Properties** button in the lower part of the window.
6. This opens a window; in that window, go to the **License keys** section.

   This section contains information about the active and reserve license keys:

   - **Serial number**: unique alphanumeric sequence.
   - **Status**: The status of the license key, for example active or reserve.
   - **Type**: type of license (commercial or trial).
   - **License validity period**: number of days during which you can use the application activated by adding this key.
   - **License limit**: number of devices on which you can use the key.
   - **Activation date** (this field is only available for the active key): date when the active key was added.
   - **License expiration date** (this field is only available for the active key): date when the application can no longer be used with the current active key.

- The Report on usage of license keys displays information about all keys added using Kaspersky Security Center. You can view the license key usage report using the Web Console (**Monitoring & Reporting** → **Reports**), as well as the Administration Console (**Reports** tab). To view the report, you need to select the "Report on usage of license keys" template in the list of reports and start generating the report.
- The Kaspersky Security Center license key store displays information about all keys added to the Kaspersky Security Center Administration Server. You can open the key store using the Web Console (**Operations** → **Kaspersky licenses**) or using the Administration Console (**Kaspersky licenses** folder).

You can also use notifications about Kaspersky Security Center events to get information about the used license keys and the licenses associated with them. The application sends information about expired licenses and license violations to the Kaspersky Security Center Administration Server.

Information about license keys on the protected device

How to view license key information on the command line

```
Viewing information about license keys and licenses on a device

kesl-control -L --query [--json]
```

Where `--json` means output data in JSON format. If you do not specify the `--json` option, settings will be output to the console.

The command outputs the following information to the console:

- Information about the active license key:
  - License expiration date and time.
  - Number of days before the end of the license term.
  - Information about the limitation of protection functionality (this line is displayed only for the key that the Kaspersky Endpoint Security application is activated with).
  - Information about limitations on updating the databases of the application.
  - Information about the status of the license key.
  - The type of license associated with the key.
  - Licensing limitation of the key (the number of licensing units).
  - Name of the application that the key is intended to activate.
  - Active license key (unique alphanumeric sequence).
  - Activation date.
- Information about the reserve license key. Displayed if the application is being used in standard mode or EDR Agent mode and a reserve key has been added If the application is being used in Light Agent mode, reserve key information is not displayed.
  - License expiration date and time.
  - Information about the limitation of protection functionality (this line is displayed only for a key that the Kaspersky Endpoint Security application may be activated with).
  - Information about limitations on updating the databases of the application.
  - Information about the status of the license key.
  - The type of license associated with the key.
  - Licensing limitation of the key (the number of licensing units).
  - Name of the application that the key is intended to activate.

- Reserve license key (unique alphanumeric sequence).
- Date and time when the license associated with the active key expires, in UTC.

You can also get information about the license under which the application is being used when viewing application details:

```
kesl-control --app-info
```

How to view license and key information in the graphical interface of the application

1. Open the main window of the application graphical interface.
2. Do one of the following:
   - In the lower part of the main window, click the area that displays information about the license and the key.
   - In the lower part of the main window, click the **Support** button to open the **Support** window, and in that window, click either the **License key** or the **Licenses** link in the lower part of the window.

   This opens the **Licenses** window.

   The window displays information about the active and reserve keys added to the application. Click the **More info** link to view full information about the licenses and keys.

The **Current licenses** section displays information about added active keys and associated licenses:

- License type, license limitation, and license term.
- **License key** – a unique alphanumeric sequence.
- **Key status** – the status of the key or a message about the problems associated with the key (if any).
- **Valid from** – date when the application was activated by adding this key.
- **Expires** – the number of days before the license expires and the license expiration date (UTC).
- **Name** – the name of the application for which the activation key was added.
- **Protection** – information about restrictions on protection functions and the ability to update application databases.

The **Reserve keys** section displays information about added reserve keys and associated licenses:

- Type of reserve key, license limit, and license term associated with the key.
- **License key** – a unique alphanumeric sequence.
- **License type** – the type of license associated with the reserve key.
- **Name** – the name of the application for which the activation key was added.
- **Protection** – information about restrictions on protection functions and the ability to update application databases.

If you use the Kaspersky Endpoint Security application in standard mode or in EDR Agent mode, and you use Kaspersky Security Center to manage the application, by default, information about license keys being added and removed and about license term expiration is recorded in the operating system log.

Management interfaces of the application

To manage Kaspersky Endpoint Security, you can use:

- Kaspersky Security Center
- The command line
- The graphical interface of the application

> You can only perform a limited subset of actions using the Kaspersky Endpoint Security graphical interface.

If Kaspersky Endpoint Security is used in Light Agent mode for protecting virtual environments, it is not possible to manage the application using Kaspersky Security Center Cloud Console and the graphical interface of the application.

If the application is being used in EDR Agent mode, only a limited subset of application component and tasks is available. You can manage certain protection components, activate the application, and update the databases. Learn more about the special aspects of the EDR Agent mode in the Known issues and limitations article.

Choose a management tool depending on the IT infrastructure of your organization, as well as the role and workflow of the administrator. We recommend managing the application on client devices remotely in a centralized fashion using Kaspersky Security Center.

Managing the application using Kaspersky Security Center

Kaspersky Security Center allows you to remotely and centrally manage the operation of Kaspersky Endpoint Security on client devices. You can remotely install and uninstall, start, and stop Kaspersky Endpoint Security; configure settings for the application, as well as for the individual components and tasks of the application; and start and stop tasks on the managed devices.

Kaspersky Security Center administration groups

To use Kaspersky Security Center to manage Kaspersky Endpoint Security installed on devices, you need to add these devices in *administration groups*. You can create administration groups in Kaspersky Security Center before Kaspersky Endpoint Security installation and configure rules to automatically move the devices to administration groups. You can also manually move the devices to the administration groups after installing the application (for details, refer to the Kaspersky Security Center Help).

Management consoles and management plug-ins

You can use the following Kaspersky Security Center administration consoles to manage Kaspersky Endpoint Security via Kaspersky Security Center:

- Kaspersky Security Center Administration Console (hereinafter also referred to as Administration Console). This is a Microsoft Management Console (MMC) snap-in that is installed on the administrator's workstation and provides a user interface for the Administration Server and Network Agent administrative services.

  The interface for managing Kaspersky Endpoint Security via the Kaspersky Security Center Administration Console is provided by the Kaspersky Endpoint Security MMC management plug-in (hereinafter also referred to as the "MMC plug-in").

  The MMC plug-in must be installed on the device where the Kaspersky Security Center Administration Console is installed.

- Kaspersky Security Center Web Console (hereinafter also referred to as *Web Console*). This is a web interface for managing a protection system based on Kaspersky applications. You can work in Kaspersky Security Center Web Console using a browser on any device.

  The interface for managing Kaspersky Endpoint Security via the Kaspersky Security Center Web Console is provided by the Kaspersky Endpoint Security management web plug-in (hereinafter also simply referred to as the web plug-in).

  The web plug-in must be installed on the device that has Kaspersky Security Center Web Console installed.

- Kaspersky Security Center Cloud Console. This is a cloud-based administration console within the cloud version of the Kaspersky Security Center application, also known as the Kaspersky Security Center Cloud Console. Interface of the Cloud console is similar to Kaspersky Security Center Web Console interface. The interface for managing Kaspersky Endpoint Security via the Kaspersky Security Center Cloud Console is also provided by the web plug-in.

  > It is not possible to manage the application using the Kaspersky Security Center Cloud Console if Kaspersky Endpoint Security is used in Light Agent mode.

> Kaspersky Endpoint Security is part of the Kaspersky Next Pro View solution. For more information about the available functionality of the application as part of this solution, see the Kaspersky Next Help.

Kaspersky Security Center policies and tasks

The MMC plug-in and web plug-in allow you to create policies and tasks in Kaspersky Security Center for managing the operation of Kaspersky Endpoint Security:

- A *policy* is a set of settings that is applied on all devices in an administration group. Policies allow you to apply identical application settings to all client devices within an administration group.

  The Kaspersky Endpoint Security policy defines the general settings for the operation of Kaspersky Endpoint Security and the settings for the operation of individual functional components of the application on devices where the policy is applied.

- *Tasks* for Kaspersky Endpoint Security created in Kaspersky Security Center run on the protected devices and implement Kaspersky Endpoint Security functions such as on-demand scan, application activation, and updates to the databases and modules of the application.

  In Kaspersky Security Center, you can create tasks to be performed on an individual device (local tasks), tasks for all devices in the administration group (group tasks), or tasks for a random selection of devices (tasks for sets of devices).

Kaspersky Security Center policies

A *policy* is a set of Kaspersky Endpoint Security settings that are applied to all client devices included in the administration group. The policy has one of the following statuses:

Policy status

Status	Description
Active	The current policy that is applied to the device.
Inactive	The policy that is not currently applied to the device.
Out-of-office	If this option is selected, the policy becomes active when the device leaves the organization network.

Policies follow these rules:

- You can configure multiple policies with different settings for one application.
- Only one policy can be active per application.
- A policy can have child policies.

Locking settings

Each policy setting has the "padlock" attribute. The status of this attribute determines whether the setting will be passed to the managed devices in the administration group.

- If the "padlock" is closed (🔒), it means the setting is applied on devices to which the policy is applied. The user cannot change such settings in the user interface of the managed application. Such settings are referred to as *locked*.
- If the "padlock" is open (🔓), it means the setting is not specified in the policy. The user can change such settings in the user interface of the managed application. Such settings are referred to as *unlocked*.

We recommend locking policy settings that you want to apply to managed devices. Unlocked policy settings can be overridden on a managed device.

The number of settings with "padlocks" in the Web Console and in the Administration Console may differ.

Policy profile

To avoid having to support a large number of policies, for example, in cases when only a few settings are supposed to be changeable, you can use policy profiles.

A *policy profile* is a set of individual policy settings that differ from the "base" policy settings and apply to client devices when the configured conditions (activation rules) are met. Using policy profiles allows you to flexibly configure application settings for different devices.

Profile settings that are locked with a "padlock" override policy settings. That is, if the profile setting locked with a "padlock" is different from the policy setting, the application applies the setting from the profile. However, lists of settings are merged, supplementing each other. That is, if the settings in the list from the profile are missing from the "basic" policy, they are added to the resulting list of settings.

Policy profiles follow these rules:

- A policy profile takes effect when a certain activation condition is satisfied.
- Policy profiles contain values of settings that are different from the values set in the policy.
- Activating a policy profile changes the effective settings of the managed device (settings that are currently applied to the device).
- A policy can have up to 100 profiles.

Settings inheritance

Policies have a hierarchy, similarly to administration groups. A *child policy* is a policy of a nested hierarchy level, that is, a policy for nested administration groups and secondary Administration Servers.

By default, a child policy inherits settings from the parent policy. If a setting in the parent policy is locked (🔒), child policies and local settings of the application get the same value, and the setting is locked. If necessary, you can disable the inheritance of settings from the parent policy. Out-of-office policies do not affect other policies through the hierarchy of administration groups.

> If the settings of the child policy are locked (*Access denied* error), check the user's access rights. If the user has the right to edit policy settings, start the *Download updates to the Administration Server repository* task for Kaspersky Security Center and repeat the authorization. This error may occur after upgrading the management plug-ins in Kaspersky Security Center: after downloading the updates, the application gets the necessary files for the new version of the management plug-in.

For some settings that have lists as values (for example, lists of rules, lists of exclusions), you can enable merging of list items. To merge list items, you need to do the following:

- In the properties of the child policy on the **General** tab, enable the **Inherit settings from parent policy** setting.
- In the properties of the parent policy, click the padlock ( ) icon to "lock" it.
- In the properties of the parent policy, enable the merging of settings by selecting the **Merge inherited values** check box. If the check box is selected, items in the list of the parent policy of Kaspersky Security Center are displayed in child policies, and items can be added to the list of child policies. If the check box is cleared, the list items are not merged when inheriting policy settings.

You cannot delete or modify inherited list items in a child policy. List items that have been merged when inherited can be deleted or modified only in the parent policy. List items can be added, modified, or removed at lower levels. Thus, you can configure a list in the parent policy, which will be applied to all child policies, and you can also add to the list in the child policy.

> If you delete an item from a list that is merged through inheritance in a parent policy, that item is not deleted from the child policies. To delete this item from the child policies, you must open the properties of those policies and delete the item manually.

Some lists are not merged. If this happens, the settings from the profile override the settings of the "base" policy:

- Exclusions by process in the File Threat Protection and Behavior Detection components
- Protection scopes in the File Threat Protection and Anti-Cryptor components
- Monitoring scopes in the System Integrity Monitoring component
- List of rules (in the **Application Control rules** window) in the Application Control component
- List of rules in Web Control
- Process memory exclusions in application settings
- Trusted domains in network settings
- Trusted root certificates in network settings
- Monitored ports in network settings
- List of SVM addresses in SVM discovery settings

After the policy is applied for the first time, the application settings change in accordance with the policy settings.

For more information about policies and policy profiles, as well as the settings inheritance mechanism, see the Kaspersky Security Center Help.

Policy management

How to create a policy in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

   A list of policies and policy profiles opens.

2. Select the administration group to which you want to apply the policy. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

3. Click **Add**.

   The Policy Wizard starts.

4. In the displayed window, select Kaspersky Endpoint Security from the list.

   Proceed to the next step of the wizard.

5. Specify the Kaspersky Endpoint Security usage mode:

   - In **Standard mode or Endpoint Detection and Response Agent mode**, the application is used to protect Linux devices as a standalone application or as an application that supports Kaspersky Detection and Response solutions and third-party anti-virus solutions working together.

     To select this mode, go to the next step of the wizard.

   - **Light Agent to protect virtual environments** – as part of the Kaspersky Security for Virtualization Light Agent solution, the application is used to protect virtual machines running Linux guest operating systems.

6. If you are using the application in Light Agent mode, configure the SVM discovery settings:

   a. Select the method that Light Agents use to discover SVMs available for connection.

      - **Use Integration Server**. If this option is selected, Light Agent connects to Integration Server to get a list of SVMs available for connection and their details.

      - **Use a custom list of SVM addresses**. If this option is selected, you can specify a list of SVMs that Light Agents managed by this policy can connect to. Light agents will only connect to SVMs specified in the list.

      If you select the **Use a custom list of SVM addresses** option, the Light Agent is using the extended SVM selection algorithm, and large infrastructure protection mode is enabled on an SVM, then connecting a Light Agent to this SVM is only possible if the SVM path is ignored. In the **SVM selection algorithm** section, you need to set the **SVM path** setting to **Ignore**. If any other value is set, Light Agents will not be able to connect to the SVM. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

b. If you select Integration Server, the wizard displays the current settings for connecting Light Agents to the Integration Server: address and port for connecting. If necessary, specify new connection settings:

a. Click the **Configure** button and specify new connection settings in the window that opens:

- **Address**. IP address in IPv4 format or fully qualified domain name (FQDN) of the device on which the Integration Server is installed. If the address is specified as a NetBIOS name, localhost or 127.0.0.1, connection to the Integration Server completes with an error.

- **Port**. Port for connecting to the Integration Server. By default, port 7271 is specified.

> If a Linux-based high-availability cluster of Integration Servers is deployed in your infrastructure, you need to specify the address and port of the load balancer as the address and port for connecting to the Integration Server. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

b. Click **Check**.

c. The web plug-in checks the SSL certificate received from the Integration Server. If the certificate contains an error or is not trusted, a corresponding message is displayed in the **Integration Server connection settings** window.

You can view information about the certificate received from the Integration Server by clicking on the **View the received certificate** line.

> If you encounter problems with an SSL certificate, we recommend to make sure that the data transmission channel you are using is secure.

To save the received certificate and continue connecting to the Integration Server, in the **Select an action** block, select the **Ignore** option.

d. Specify the password of the Integration Server administrator (password of the `admin` account) and click the **Test** button.

The New Policy Wizard connects to the Integration Server. If the connection fails, an error message appears in the window. If the connection succeeds, the **Connection to the Integration Server** window closes, and the **Connection to the Integration Server** field of the New Policy Wizard window shows the **Connected** status.

c. If you select a manually defined list of SVM addresses, create a list of SVMs that Light Agents managed by this policy can connect to. To add an SVM to the list, click the **Add** button and, in the window that opens, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line.

> Specify only fully qualified domain names (FQDNs) that map to a single IP address. Using a fully qualified domain name that corresponds to multiple IP addresses can lead to errors in the application.

You can delete addresses selected in the list by clicking the **Delete** button.

Proceed to the next step of the wizard.

7. Decide whether you want to use Kaspersky Security Network. Carefully read the Kaspersky Security Network Statement and do one of the following:

   - If you agree with all terms and conditions of the Statement and want to use Kaspersky Security Network with the application, select **I agree to use Kaspersky Security Network**.

   - If you do not want to use Kaspersky Security Network, select **I do not agree to use Kaspersky Security Network** and confirm your decision in the window that opens.

   Refusal to use Kaspersky Security Network does not interrupt the policy creation process. At any time, you can enable or disable use of Kaspersky Security Network or change the KSN mode for managed devices in the policy settings.

   Proceed to the next step of the wizard.

8. You will be prompted to read the recommendations for configuring Kaspersky Endpoint Security. Review the settings that allow optimizing the usage of system resources by the application.

   Proceed to the next step of the wizard.

9. The **General** tab of the new policy settings window opens. Specify a name for the new policy.

   You can also configure the following policy settings:

   - Policy status:

     - **Active**. The policy that is currently applied to the device. If this option is selected, this policy becomes active on the device upon the next device synchronization with the Administration Server. This option is selected by default.

     - **Inactive**. If this option is selected, the policy is not applied to the device, but remains in the **Policies** folder. You can activate the inactive policy later.

     - **Out-of-office**. If this option is selected, the policy becomes active when the device leaves the organization network.

       In the Network Agent policy that is active on the device, in the **Network** → **Connection profiles** section, the **Enable out-of-office mode when Administration Server is not available** setting must be enabled.

   - Policy settings inheritance:

     - **Inheritance from parent policy**. If this toggle switch is enabled, the policy settings are inherited from the upper-level group policy. Settings that are locked with a "padlock" (🔒) in the parent policy are not editable. The toggle switch is switched on by default.

     - **Forced inheritance for child policies**. If this toggle switch is enabled, the policy settings are propagated to child policies. In the properties of the child policy, the **Inheritance from parent policy** toggle button will be automatically switched on and cannot be switched off. The settings of the child policy are inherited from the parent policy, except for the settings for which the "padlock" (🔓) is open. The toggle button is switched off by default.

   For general information about the policy settings, refer to the Kaspersky Security Center Help.

10. If you want to manage other policy settings, go to the **Application settings** tab and make changes as necessary.

    You can also change the policy settings later.

11. Click the **Save** button.

How to create a policy in the Administration Console

1. In the Administration Console tree, in the **Managed devices** folder, select the administration group containing the devices to which the policy should be applied.

   You can view the list of devices that are part of an administration group on the **Devices** tab of the folder with the name of this administration group.

2. In the workspace, select the **Policies** tab.

3. Click the **New policy** button to start the New policy wizard.

   You can also start the Wizard by clicking the **Create** → **Policy** item in the context menu in the list of policies.

4. At the first step of the wizard, in the list, select Kaspersky Endpoint Security.

   Proceed to the next step of the wizard.

5. Enter a name for the new policy.

6. To use the settings from the previous version of Kaspersky Endpoint Security policy in the policy being created, select the **Use policy settings for the earlier application version** check box.

   Proceed to the next step of the wizard.

7. Decide whether you want to use Kaspersky Security Network. Carefully read the Kaspersky Security Network Statement and do one of the following:

   - If you agree with all the terms and conditions of the Statement and want the application to use Kaspersky Security Network, select **I confirm that I have fully read, understand, and accept the terms and conditions of Kaspersky Security Network Statement**.

   - If you do not want to use Kaspersky Security Network, select **I do not accept the terms and conditions of the Kaspersky Security Network Statement** and confirm your decision in the window that opens.

   Refusal to use Kaspersky Security Network does not interrupt the policy creation process. At any time, you can enable or disable use of Kaspersky Security Network or change the KSN mode for managed devices in the policy settings.

   Proceed to the next step of the wizard.

8. Specify the Kaspersky Endpoint Security usage mode:

   - In **Standard mode or Endpoint Detection and Response Agent mode**, the application is used to protect Linux devices as a standalone application or as an application that supports Kaspersky Detection and Response solutions and third-party anti-virus solutions working together.

   - **Light Agent mode for protecting virtual environments** – as part of the Kaspersky Security for Virtualization Light Agent solution, the application is used to protect virtual machines running Linux guest operating systems.

   Proceed to the next step of the wizard.

9. If you are using the application in Light Agent mode, configure the SVM discovery settings:

   a. Select the method that Light Agents use to discover SVMs available for connection.

      - **Use Integration Server**. If this option is selected, Light Agent connects to Integration Server to get a list of SVMs available for connection and their details.

      - **Use a custom list of SVM addresses**. If this option is selected, you can specify a list of SVMs that Light Agents managed by this policy can connect to. Light agents will only connect to SVMs specified in the list.

      If you select the **Use a custom list of SVM addresses** option, the Light Agent is using the extended SVM selection algorithm, and large infrastructure protection mode is enabled on an SVM, then connecting a Light Agent to this SVM is only possible if the SVM path is ignored. In the **SVM selection algorithm** section, you need to set the **SVM path** setting to **Ignore**. If any other value is set, Light Agents will not be able to connect to the SVM. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

   b. If you select Integration Server, the wizard displays the current settings for connecting Light Agents to the Integration Server: address and port for connecting. If necessary, specify new connection settings:

      a. Click the **Edit** button and specify new connection settings in the window that opens:

         - **Address**. IP address in IPv4 format or fully qualified domain name (FQDN) of the device on which the Integration Server is installed. If the address is specified as a NetBIOS name, localhost or 127.0.0.1, connection to the Integration Server completes with an error.

         - **Port**. Port for connecting to the Integration Server. By default, port 7271 is specified.

         If a Linux-based high-availability cluster of Integration Servers is deployed in your infrastructure, you need to specify the address and port of the load balancer as the address and port for connecting to the Integration Server. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

      b. Click **OK**.

      c. If the device hosting the Kaspersky Security Center Administration Console does not belong to a domain or your account does not belong to the KLAdmins local or domain group or to the local administrator group, the Integration Server administrator account is used for authentication on the Integration Server.

         In the window that opens, enter the password of the Integration Server administrator (password of the `admin` account) and click the **OK** button.

      d. The MMC plug-in checks the SSL certificate received from the Integration Server. If the certificate contains an error or is not trusted, the **Verify Integration Server certificate** window opens. You can click the link in the window to view the details of the received certificate.

         If you encounter problems with an SSL certificate, we recommend to make sure that the data transmission channel you are using is secure.

To continue connecting to the Integration Server, click the **Ignore** button. The received certificate will be installed as a trusted certificate on the device where the Kaspersky Security Center Administration Console is installed.

c. If you select a manually defined list of SVM addresses, create a list of SVMs that Light Agents managed by this policy can connect to. To add an SVM to the list, click the **Add** button and, in the window that opens, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line.

> Specify only fully qualified domain names (FQDNs) that map to a single IP address. Using a fully qualified domain name that corresponds to multiple IP addresses can lead to errors in the application.

You can delete addresses selected in the list by clicking the **Delete** button.

Proceed to the next step of the wizard.

10. If necessary, configure the general settings for File Threat Protection.

    Proceed to the next step of the wizard.

11. If necessary, edit the File Threat Protection settings that have been configured by default.

    Proceed to the next step of the wizard.

12. If necessary, configure the exclusions from File Threat Protection.

    Proceed to the next step of the wizard.

13. If necessary, modify the default actions for infected objects.

    Proceed to the next step of the wizard.

14. Select a policy state:

    - **Active policy**. The policy that is currently applied to the device. If this option is selected, this policy becomes active on the device upon the next device synchronization with the Administration Server. This option is selected by default.
    - **Inactive policy**. If this option is selected, the policy is not applied to the device, but remains in the **Policies** folder. You can activate the inactive policy later.
    - **Out-of-office policy**. If this option is selected, the policy becomes active when the device leaves the organization network.

    > In the Network Agent policy that is active on the device, in the **Network** → **Connection profiles** section, the **Enable out-of-office mode when Administration Server is not available** setting must be enabled.

15. Complete the New Policy Wizard.

    The created policy is displayed in the list of policies of the administration group on the **Policies** tab and in the **Policies** folder of the console tree.

For general information about managing policies, refer to the Kaspersky Security Center Help.

Useful articles

What to do if tasks do not run or policies are not applied

What to do if the device has the status: "Invalid policy settings. Policy has not been applied."

Error: "Application is not supported by the current version of Kaspersky Security Center Web Console or application web plug-in is not installed"

Exporting and importing policy settings

Kaspersky Endpoint Security allows exporting a policy with its settings and profiles to a KLP file. You can then use the policy export / import functionality to back up policies, migrate policies to another server or, for example, to migrate policies from Kaspersky Security Center Windows to Kaspersky Security Center Linux. For details on managing policies, please refer to the Kaspersky Security Center Help.

How to export and import a policy in the Administration Console (MMC)

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the workspace, select the **Policies** tab.
4. To export a policy:
   a. Click the policy you want to export.
   b. Click the **Export policy to file** link in the right part of the window.
   c. In the window that opens, specify the name of the KLP file to which you want to export the policy, and select the folder to save the file.
   d. Save the file.
5. To import a policy:
   a. Click **Import policy from file**.
   b. In the window that opens, select the KLP policy file that you want to import.
   c. Open the file.

   This adds a new policy with the *Inactive policy* status.

How to export and import the policy in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. To export a policy:
   a. Select the check box next to the policy that you want to export.
   b. Click the **Export** button.
   c. In the window that opens, specify the name of the KLP file to which you want to export the policy, and select the folder to save the file.
   d. Save the file.
3. To import a policy:
   a. Click **Import**.
   b. Select the KLP policy file that you want to import.
   c. After the policy is successfully processed, select the administration group to which you want to apply the policy.
   d. Click the **Complete** button to finish importing the policy.

   This adds a new policy with the *Inactive* status.

Exporting and importing certain policy settings in the Web Console

In the Web Console, you can export individual policy settings to a JSON file and import such settings from a file. For example, you can export a list of Web Control rules or File Threat Protection scopes.

The following settings are available for export and import:

- File Threat Protection scopes
- Attachment filters of Mail Threat Protection
- Network packet rules
- Web Control rules
- Application Control rules
- Monitoring scopes and System Integrity Monitoring exclusion scopes
- Telemetry settings
- Certain Trusted Zone exclusions

To export or import settings in the Web Console:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the section from which you want to export or import settings.
5. Click the button.
6. Select an action: **Import** or **Export**.
7. If you are importing settings, select the file from which you want to import settings.

Tasks for Kaspersky Endpoint Security created in Kaspersky Security Center

You can create the following types of tasks in Kaspersky Security Center for Kaspersky Endpoint Security:

- local tasks to run on individual devices;
- group tasks to run on devices within an administration group;
- Tasks for the selection of devices to run on multiple devices, regardless of their inclusion in administration groups.

You can create any number of tasks.

General information about tasks created in Kaspersky Security Center is provided in Kaspersky Security Center Help.

Task types

The following tasks are provided for managing Kaspersky Endpoint Security in Kaspersky Security Center:

- *Malware Scan*. During the task execution, the application scans the device areas that are specified in the task settings for viruses and other malware.
- *Critical Areas Scan*. During the task execution, the application scans boot sectors, startup objects, process memory, and kernel memory.
- *Container Scan*. During the task execution, the application scans containers and images for viruses and other malware.
- *Inventory*. During the task execution, the application receives information about all executable files stored on the devices and manages the Golden Image.

- *System Integrity Check*. During the task execution, the application determines changes of each object by comparing the current state of the monitored object to its original state, which was previously established as a baseline.

- *Add Key*. During the task execution, the application adds a key, including a reserve one, to activate the application.

- *Update*. During the task execution, the application updates the databases in accordance with the configured update settings.

- *Rollback*. During the task execution, the application rolls back the last database update.

Managing tasks in the Web Console

How to create a task for a group or selection of devices in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** → **Tasks**.

   The list of tasks opens.

2. Click the **Add** button.

   The Task Wizard starts.

3. In the first step of the Wizard, perform the following actions:

   a. In the **Application** drop-down list, select the application name: Kaspersky Endpoint Security.

   b. In the **Task type** drop-down list, select the type of task that you want to create.

   c. In the **Task name** field, enter a name for the new task.

   d. In the **Devices to which the task will be assigned** section, select the method for defining the task scope. The task scope comprises the devices on which the task will be run:

      - Select the **Assign task to an administration group** option if the task is to be run on all devices included in a specific administration group.

      - Select the **Specify device addresses manually, or import addresses from a list** option if the task is to be run on the specified devices.

      - Select the **Assign task to a device selection** option if the task is to be run on devices included in the device selection according to a predefined criterion. For information on how to create a device selection, refer to the Kaspersky Security Center Help system.

   Proceed to the next step of the wizard.

4. Depending on the selected method for defining the task scope, perform one of the following actions:

   - In the administration group tree, select the check boxes next to the required administration groups.
   - In the list of devices, select the check boxes next to the required devices. If the required devices are not listed, you can add them in the following ways:
     - Using the **Add devices** button. You can add devices by name or IP address, add devices from a specified IP range, or select devices from the list of devices detected by the Administration Server when polling the corporate LAN.
     - Using the **Import devices from file** button. For the import, a TXT file with a list of device addresses is used, where each address must be on a separate line.
   - From the list, select the name of the selection containing the required devices.

   Proceed to the next step of the wizard.

5. To manage task settings immediately after creating the task, at the last step of the wizard, select the **Open task details when creation is complete** check box. A task is created with the default settings.

6. Finish the wizard.

A new task will be displayed in the list of tasks.

How to create a local task in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To do so, click the **Show hierarchy** button above the list of managed devices and select an administration group in the window that opens.

   The list displays only the managed devices for the selected administration group.

3. In the list, find the device for which you want to create a task and click the device name.

4. This opens a managed device properties window; in that window, go to the **Tasks** tab.

   The list of tasks created for this device is displayed.

5. Click the **Add** button.

   The Task Wizard starts.

6. In the first step of the Wizard, perform the following actions:

   a. In the **Application** drop-down list, select the application name: Kaspersky Endpoint Security.

   b. In the **Task type** drop-down list, select the type of task that you want to create.

   c. In the **Task name** field, enter a name for the new task.

7. To manage task settings immediately after creating the task, at the last step of the wizard, select the **Open task details when creation is complete** check box. A task is created with the default settings.

8. Finish the wizard.

A new task will be displayed in the list of tasks.

How to start, stop, pause, or resume a task in the Web Console

1. In the main window of Kaspersky Security Center Web Console, select **Assets (Devices)** → **Tasks**.

   The list of tasks opens.

2. Do one of the following:

   - To start or stop a task that is run on all devices included in a certain administration group, click the **Show hierarchy** button in the upper part of the window and select the administration group in the window that is displayed.

     The list displays only the tasks created for the selected administration group.

   - To start or stop a task that is run on one or multiple devices (a task for a set of devices), click the **Show hierarchy** button in the upper part of the window and select the top node with the name of the Administration Server in the window that is displayed.

     The list displays all tasks created on the Administration Server.

3. In the list of tasks, check the box next to the name of the required task and click the action button above the list of tasks.

   The *Update* task cannot be paused or resumed, it can only be started or stopped.

Managing tasks in the Administration Console

To create a task for a group or selection of devices in the Administration Console

1. In the Administration Console, perform one of the following actions:

   - To create a task that will be run on devices included in the selected administration group, select this administration group in the console tree in the **Managed devices** folder, then select the **Tasks** tab in the workspace and click the **New task** button.

     The New task wizard starts for devices of the selected administration group.

   - To create a task that will be performed on one or multiple devices (a task for a set of devices), select the **Tasks** folder in the console tree and click the **New task** button in the workspace.

     The New task wizard starts for the set of devices.

2. At the first step of the wizard, select Kaspersky Endpoint Security and a task type.

   Proceed to the next step of the wizard.

3. If you are creating a task for a set of devices, the Wizard prompts you to define the task scope. The task scope comprises the devices on which the task will be run.

   a. Specify the method for defining the task scope: select devices from the list of devices detected by the Administration Server; set device addresses manually; import a list of devices from a file or specify a previously configured selection of devices (for more details, refer to the Kaspersky Security Center Help).

   b. Depending on the method you have specified for defining the task scope, in the window that opens, perform one of the following actions:

      - In the list of detected devices, specify the devices on which the task will be run. To do so, select the check box in the list to the left of the device name.
      - Click the **Add** or **Add IP range** button and enter the device addresses manually.
      - Click the **Import** button and select the TXT file containing the list of device addresses in the window that opens.
      - Click the **Browse** button and, in the window that opens, specify the name of the selection containing the devices on which the task will be run.

   Proceed to the next step of the wizard.

4. Configure the available task settings by following the instructions in the Wizard.

5. Enter the name of the new task and proceed to the next step in the Wizard.

6. To start the task immediately after the Wizard finishes, in the final step, select the **Run task after the wizard finishes** check box.

7. Finish the wizard.

   A new task will be displayed in the list of tasks.

How to create a local task in the Administration Console

1. In the Administration Console tree, in the **Managed devices** folder, select the administration group containing the necessary device.

2. In the workspace, select the **Devices** tab.

3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.

4. In the displayed window with the properties of the managed device, select the **Tasks** section.

   The list of tasks created for this device is displayed.

5. Click the **Add** button.

   The Task Wizard starts.

6. At the first step of the wizard, select Kaspersky Endpoint Security and a task type.

   Proceed to the next step of the wizard.

7. Enter a name for the new task and configure the available task settings following the instructions of the wizard.

8. Finish the wizard.

   A new task will be displayed in the list of tasks.

How to start, stop, pause, or resume a task in the Administration Console

1. In the Administration Console, perform one of the following actions:

   - To start or stop a task that is run on devices included in the specified administration group, select this administration group in the console tree, then select the **Tasks** tab in the workspace.

     The list of tasks created for the selected administration group opens.

   - To start or stop a task that is run on one or multiple devices (a task for a set of devices), select the **Tasks** folder in the console tree.

     The list of all tasks created on the Administration Server opens.

2. In the list of tasks, select the required task, open the context menu of the task, and select the action that you want to perform.

   > The *Update* task cannot be paused or resumed, it can only be started or stopped.

In the list of tasks, you can monitor the task execution results: view the task status and the statistics for task performance on the devices. You can also create a selection of events to monitor the execution of tasks. For more details on event selection, please refer to the Kaspersky Security Center Help.

Task execution results are also saved locally on the device and in Kaspersky Security Center reports.

Special considerations involved in managing and running tasks

- The task for the sets of devices is performed only on the devices that are specified in the task. If new devices are added to the set of devices for which a task has been created, that task will not be executed for those devices. In this case, you need to create a new task or edit the existing one.

- The tasks are executed only if Kaspersky Endpoint Security is running on the devices.

- If the device is managed by a policy, it may not be possible to view and manage tasks created in Kaspersky Security Center using the command line or the graphical interface of the application.

- For the Kaspersky Endpoint Security application in Kaspersky Security Center, you can create all types of tasks. Applying and running tasks on a protected device is determined by the mode of the application on the device. For example, the *Add Key*, *Update*, and *Rollback* tasks are not applied on the device if the application is running in Light Agent mode.

Logging in and out of the Web Console and Cloud Console

Kaspersky Security Center Web Console

To log in to the Web Console, you need to know the web address and the port number of the Administration Server specified during the Web Console installation (port 8080 is used by default). JavaScript must also be enabled in your browser.

You can log in to the Kaspersky Security Center Web Console by using one of the following methods:

- Domain authentication (Single Sign-On)
- User name and password of a domain user
- User name and password of an internal user

For more details on logging in and out of the Kaspersky Security Center Web Console, see the Kaspersky Security Center Help.

To log in to the Web Console by specifying a user name and password:

1. In your browser, go to:

   ```
   https://<Kaspersky Security Center Web Console address>:<port number>
   ```

   This opens the page for selecting the Administration Server.

2. If you have added multiple trusted administration servers, select the Administration Server to which you want to connect from the list.

   If you have added only one Administration Server, the list of Administration Servers is not displayed.

   The browser is redirected to `https://<Administration Server address>:4444`.

3. Enter the user name and password for your account.

   > It is recommended to make sure that the password complexity and anti-bruteforce mechanisms ensure that the password cannot be guessed within 6 months.

4. Click **Log in**.

   If the Administration Server is not responding, or if you enter incorrect credentials, an error message is displayed.

5. Enter the one-time security code generated in the authentication app on your mobile device.

   If logging in for the first time, configure 2-step authentication for your account.

After logging in, a dashboard is displayed with the last language and theme used.

For more details about the Web Console interface, see the Kaspersky Security Center Help.

To log out of Web Console:

select **<Account name>** → **Exit** in the lower left corner of the screen.

The Web Console is closed, and the login page is displayed.

Kaspersky Security Center Cloud Console

For the Kaspersky Security Center Cloud Console, use a web token to log in to your account on the Cloud Console portal.

For detailed information about Kaspersky Security Center Cloud Console, refer to Kaspersky Security Center Cloud Console documentation.

Managing the application using the command line

Using the command line, you can install, uninstall, start, and stop Kaspersky Endpoint Security on the device, and also manage the application locally.

Components and tasks

The functional components of the application are supported by *Kaspersky Endpoint Security local tasks* that are run in the operating system. To enable or disable a functional component of the application on a device, you need to start or stop the corresponding Kaspersky Endpoint Security task on the command line.

To scan a device once, you also need to start the corresponding Kaspersky Endpoint Security task.

To manage the settings of a functional component on a device or settings for scanning a device, you need to manage the settings of the corresponding Kaspersky Endpoint Security task.

General settings

In addition to settings specific to individual Kaspersky Endpoint Security tasks, there are some general settings:

- General Container Scan settings. Used when scanning containers and namespaces in real time (Container Monitoring).
- Network traffic scan settings. Used by the Web Threat Protection, Network Threat Protection, Mail Threat Protection, and Web Control components.
- General application settings. These settings govern the operation of the application as a whole and the operation of individual functions.

Management commands

You can manage Kaspersky Endpoint Security tasks and settings on the command line using *kesl-control utilities*.

Only user tasks can be created or deleted. Predefined tasks cannot be created or deleted.

Depending on the mode of the application, you can create the following types of user tasks:

- Standard mode: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan*, and *InventoryScan*;
- Light Agent mode: *ODS*, *ODFIM*, *ContainerScan*, and *InventoryScan*.

You can start and stop all predefined tasks and user tasks except tasks of the *License* type.

You can suspend and resume *ODS*, *ODFIM*, and *InventoryScan* tasks.

Kaspersky Endpoint Security local tasks

The following tasks can be used for managing Kaspersky Endpoint Security on the command line, as listed in the table below:

Each application task has a name used on the command line, an ID, and a type.

IDs are unique for all tasks, including deleted tasks. The application does not reuse the identifiers of the deleted tasks. The identifier of a new task is the next successive number to the identifier of the latest created task.

Task names are not case-sensitive.

During installation of the application, *predefined tasks* are created. These tasks cannot be deleted. Each predefined task has a name and ID.

Tasks that you create while working with the application are called *user tasks*. When you create the task, you specify the name for it. IDs for user tasks are defined and assigned by the application when the task is created. IDs for user tasks are starting from 100.

During operation, the application creates *temporary scan tasks*. Temporary task names and IDs are assigned by the application. Temporary tasks are automatically deleted when completed.

Application tasks

Task	Task description	Task name in command line	Task ID	Task type
File Threat Protection	This task allows you to enable or disable File Threat Protection in real time and defines the settings for the File Threat Protection component. If File Threat Protection is enabled, the task runs automatically at application startup	File_Threat_Protection	1	OAS
Malware Scan	This task allows you to scan file system objects for malware on demand and defines the settings for the scan. You can use this task to perform a full or custom scan of the device.	Scan_My_Computer	2	ODS
Malware Scan (user task)		user-defined	starting from 100	ODS

Task	Task description	Task name in command line	Task ID	Task type
Custom file scan	This task is designed for configuring and storing settings that are used when scanning the specified files and directories using the `kesl-control --scan-file` command. As a result of the command execution, the application creates and starts a temporary file scan task.	Scan_File	3	ODS
Critical Areas Scan	This task allows you to run a critical areas scan of the operating system on demand and defines the settings for the scan.	Critical_Areas_Scan	4	ODS
Update	You can use this task to perform scheduled and on-demand application database and module updates and edit update settings.	Update	6	Update
Update (user task)		user-defined	starting from 100	Update
Rollback	You can use this task to roll back the last update of application databases and modules.	Rollback	7	Rollback
Rollback (user task)		user-defined	starting from 100	Rollback
Licensing	This task provides the capability to activate an application installed on the device. The task starts automatically when the application starts, and it resides in the device operating memory. The task has no settings; license keys are managed using special management commands. The task cannot be started, stopped, or deleted.	License	9	License
System Integrity Check	This task allows you to check for changes in files and directories that you have included in the monitoring scope, by comparing the current state of the monitored object with a previously recorded state.	System_Integrity_Monitoring	11	OAFIM
System Integrity Check (user task)		user-defined	starting from 100	ODFIM
Firewall Management	This task allows you to enable or disable firewall management and defines the network connection control settings on the device.	Firewall_Management	12	Firewall
Anti-Cryptor	This task allows you to enable or disable the protection of files from remote malicious encryption and defines the settings for the Anti-Cryptor component.	Anti_Cryptor	13	AntiCryptor
Web Threat Protection	This task allows you to enable or disable Web Threat Protection and defines the settings for the Web Threat Protection component. If Web Threat Protection is enabled, the task runs automatically on application startup	Web_Threat_Protection	14	WTP
Device Control	This task allows you to enable or disable Device Control and defines the settings for the Device Control component. If Device Control is enabled, the task runs automatically on application startup.	Device_Control	15	DeviceControl
Removable Drives Scan	This task allows you to monitor the connection of removable media to the device in real time and defines the settings of the Removable Drives Scan and the scan of its boot sectors for malware.	Removable_Drives_Scan	16	RDS
Network Threat Protection	This task allows you to enable or disable Network Threat Protection and defines the settings for the Network Threat Protection component.	Network_Threat_Protection	17	NTP

Task	Task description	Task name in command line	Task ID	Task type
Container Scan	This task allows you to scan containers and images on demand and defines the settings for the scan.	Container_Scan	18	ContainerScan
Container Scan (user task)		user-defined	starting from 100	ContainerScan
Custom Container Scan	This task is designed for configuring and storing settings that are used when scanning the specified containers and images using the `kesl-control [-T] --scan-container` command. As a result of the command execution, the application creates and starts a temporary Container Scan task.	Custom_Container_Scan	19	ContainerScan
Behavior Detection	This task allows you to monitor malicious activity of applications in the operating system. If Behavior Detection is enabled, the task runs automatically on application startup.	Behavior_Detection	20	BehaviorDetection
Application Control	This task allows you to enable or disable Application Control and defines the settings of the Application Control component.	Application_Control	21	AppControl
Inventory	This task allows getting information about all executable files of applications on the device and managing the Golden Image category of applications.	Inventory_Scan	22	InventoryScan
Inventory (user task)		user-defined	starting from 100	InventoryScan
Kaspersky Endpoint Detection and Response Expert (on-premises) Integration.	This task allows enabling or disabling the integration with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA) and managing integration settings.	KATAEDR	24	KATAEDR
Web Control	This task allows you to enable or disable Web Control and defines the settings of the Web Control component.	Web_Control	26	WebControl
Sandbox Integration	This task enables and disables integration with Sandbox and specifies the integration settings.	Standalone_Sandbox	29	StandaloneSandbox
Execution Prevention for objects (EDR Expert (on-premises))	This task lets you enable and disable the use of Endpoint Detection and Response Expert (on-premises) execution prevention rules and also view a list of these rules.	KATAEDR_Prevention	30	KATAEDRPrevention
Kaspersky Network Detection and Response (KATA) Integration	This task allows you to enable or disable integration with Kaspersky Network Detection and Response (KATA) and specifies the integration settings.	KATANDR	31	KATANDR
Execution prevention for objects (EDR Optimum)	This task lets you enable and disable the use of Endpoint Detection and Response Optimum execution prevention rules and also view a list of these rules.	EDRO_Prevention	32	Prevention
KUMA Integration	This task enables and disables integration with Kaspersky Unified Monitoring and Analysis Platform and specifies the integration settings.	KUMA	33	KUMA
Mail Threat Protection	This task allows you to scan the attachments of incoming and outgoing email messages for viruses and other threatening applications. If Mail Threat Protection is enabled, the task runs automatically on application startup	Mail_Monitoring	35	MailMonitoring

Task	Task description	Task name in command line	Task ID	Task type
BadUSB Attack Prevention	This task allows you to prevent the connection of infected USB devices that imitate a keyboard to a client device.	Bad_USB	37	BadUSB
Kaspersky Endpoint Detection and Response Expert (cloud) integration	This task allows you to enable or disable integration with Kaspersky Endpoint Detection and Response Expert (cloud) and specifies the integration settings.	EDRExpertCloud	39	EDRExpertCloud

Editing task settings

You can edit the settings for all user tasks and all predefined tasks, except for tasks of the *Rollback* and *License* types (these tasks have no settings). If the application is used in Light Agent mode, the settings of the predefined *Update* task also cannot be edited.

For tasks of the *OAS*, *ODS*, *OAFIM*, *ODFIM*, and *AntiCryptor* types, you can add or remove scan scopes and exclusion scopes.

You can edit task settings in the following ways:

- Using a configuration file. This method allows modifying all task settings at the same time. You can get a configuration file to edit using the command that outputs task settings.
- Using command line options in the <setting name>=<setting value> format. This method allows changing individual task settings. You can view the current values of task settings using the command that outputs task settings.

For some tasks, separate management commands are also provided that allow you to edit task settings.

How to output the current values of task settings

You can output the current values of task settings to the console or to a configuration file. You can then edit this file to modify the task settings.

```
Output the current values of the task settings to the console

kesl-control --get-settings <task ID|name>
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

```
Output the current values of the task settings to a configuration file

kesl-control --get-settings <task ID/name> --file <path to configuration file> [--json]
```

Where:

- `--file <path to configuration file>` is the path to the configuration file to which you want to output the task settings. If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, the configuration file will not be created.

- `--json` is specified to output the settings in JSON format. If the `--json` option is not specified, the settings are output in the INI format.

How to modify task settings using a configuration file:

1. Output the task settings to the configuration file using the following command:

   ```
   kesl-control --get-settings --file <path to configuration file> [--json]
   ```

   where:

   - `--file <path to configuration file>` is the full path to the configuration file from which you want to import the task settings.

   - Specify the `--json` option if you want to output the settings to a JSON configuration file. If the `--json` options is not specified, the application will output the settings to an INI file.

2. Open the resulting configuration file, edit the settings as necessary, and save your changes.

   For tasks of the *OAS*, *ODS*, *OAFIM*, *ODFIM*, and *AntiCryptor* types, you can add or remove scan scopes and exclusion scopes.

   If you want to add a scan scope, add a `[ScanScope.item_#]` section with the following settings to the file:

   - `AreaDesc` is a description of the scan scope, which contains additional information about this scope.

   - `UseScanArea` enables scanning of the specified scope.

   - `Path` is a path to the directory with the objects to be scanned. You can specify a path to a local directory or enable scanning of remote directories mounted on a client device.

   - `AreaMask.item_#` is a limitation of the scan scope. You can specify a mask for the name of the files to be scanned. Scanning is enabled by default for all objects in the scan scope. You can specify multiple `AreaMask.item_#` items.

   If you want to add an exclusion scope, add an `[ExcludedFromScanScope.item_#]` section with the following settings to the file:

   - `AreaDesc` – a description of the exclusion scope, which contains additional information about the exclusion scope.

   - `UseScanArea` enables exclusion of the specified scope.

   - `Path` is a path to the directory with the objects to be excluded. You can specify a path to a local directory or exclude remote directories mounted on a client device. Possible values for the setting depend on the type of task.

- `AreaMask.item_#` is a limitation of the exclusion scope. You can specify a mask for the name of the files that you want to exclude from the scan scope. By default, all objects in the scope are excluded.

  Example

  ```
  [ExcludedFromScanScope.item_0000]
  AreaDesc=
  UseScanArea=Yes
  Path=/tmp/notchecked
  AreaMask.item_0000=*
  ```

You can specify multiple `[ScanScope.item_#]` and `[ExcludedFromScanScope.item_#]` sections. The application processes the scopes by index in ascending order.

3. Run the following command:

   ```
   kesl-control --set-settings <task ID/name> --file <path to configuration file> [--json]
   ```

   where:

   - `<task ID/name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
   - `--file <path to configuration file>` is the full path to the configuration file from which you want to import the task settings.
   - Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

   All values of task settings defined in the file will be imported into the application.

If you change the allowlist, or prohibit launch of all applications or applications that affect the operation of Kaspersky Endpoint Security in the Application Control task settings, run the `--set-settings` command with the `--accept` option.

How to change individual task settings using command line options

Execute the command:

```
kesl-control --set-settings <task ID|name> <setting name >=<setting value> [<setting name >=<setting value>]
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `<setting name >=<setting value>` is the name and value of one task setting. You can get the current values of task settings using the command for displaying task settings.

The values of the specified task settings will be changed.

> If you change the allowlist, or prohibit launch of all applications or applications that affect the operation of Kaspersky Endpoint Security in the Application Control task settings, run the `--set-settings` command with the `--accept` option.

How to add or remove a scan scope using command line options

Add a scan scope using command line options

```
kesl-control --set-settings <task ID|name> --add-path <path>
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `<path>` is a path to the directory with the objects to be scanned.

This command adds a new `[ScanScope.item_#]` section to task settings. The application scans the objects in the directory specified by the `Path` setting. The remaining settings of the scan scope take default values.

If the task settings already contain an `[ScanScope.item_#]` section with the specified value for the `Path` setting, a duplicate section is not added.

If the `UseScanArea` setting is set to `No` its value will change to `Yes` after this command is executed and the objects located in this directory will be scanned.

Example of adding the /home directory to the scan scope for a task with ID=100

```
kesl-control --set-settings 100 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/home
```

The following scan scope settings will be added to the task:

```
[ScanScope.item_0001]
AreaDesc=
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

Remove a scan scope using command line options

```
kesl-control --set-settings <task ID|name> --del-path <path>
```

This command removes the `[ScanScope.item_#]` section, which contains the specified path, from task settings. The application will not scan the objects in the specified directory.

How to add or remove an exclusion scope using command line options

Add an exclusion scope using command line options

```
kesl-control --set-settings <task ID|name> --add-exclusion <path>
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `<path>` is a path to the directory with the objects to be excluded.

This command adds a new `[ExcludedFromScanScope.item_#]` section to task settings. The application will exclude objects in the directory specified by the `Path` setting from scans. The remaining settings of the exclusion scope take default values.

If the task settings already contain an `[ExcludedFromScanScope.item_#]` section with the specified value for the `Path` setting, a duplicate section is not added.

If the `UseScanArea` setting is set to `No` its value will change to `Yes` after this command is executed and the objects located in this directory will be excluded from scans.

```
Remove an exclusion scope using command line options

kesl-control --set-settings <task ID|name> --del-exclusion <path>
```

This command removes the `[ExcludedFromScanScope.item_#]` section, which contains the specified path, from task settings. The application will not exclude the objects in the specified directory from the scan.

How to restore default task settings

Execute the command:

```
kesl-control --set-settings <task ID|name> --set-to-default
```

Where `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

The application changes the setting values to their defaults.

Configuring the task schedule

Depending on the mode of the application, you can configure a schedule for the following types of tasks:

- Standard mode: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan*, and *InventoryScan*;
- Light Agent mode: *ODS*, *ODFIM*, *ContainerScan*, and *InventoryScan*.

You can edit the task schedule in the following ways:

- Using a configuration file. This method allows modifying all the task schedule settings at the same time. You can get a configuration file to edit using the command that outputs schedule settings.
- Using command line options in the <setting name>=<setting value> format. This method allows modifying individual task schedule settings. You can view the current values of task settings using the command that outputs schedule settings.

How to output the current schedule settings

You can output the current values of the settings for the task run schedule to the console or to a configuration file. You can then edit this file to modify the settings.

```
Output the current task schedule settings to the console
```

```
kesl-control --get-schedule <task ID|name> [--json]
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `--json` is specified to output the settings in JSON format. If the --json option is omitted, the settings are output in the INI format.

```
Output the current task schedule settings to a configuration file
```

```
kesl-control --get-schedule <task ID|name> --file <path to configuration file> [--json]
```

Where `--file <path to configuration file>` is the path to the configuration file to which you want to output the task schedule settings. If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, the configuration file will not be created.

```
Example of output of the update task schedule settings to a file named update_schedule.ini and saving the created file to the current directory
```

```
kesl-control --get-schedule 6 --file update_schedule.ini
```

```
Example of writing the update task schedule to the terminal
```

```
kesl-control --get-schedule 6
```

How to configure the task schedule using a configuration file

```
kesl-control --set-schedule <task ID|name> --file <path to configuration file> [--json]
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `--file <path to configuration file>` is the full path to the configuration file from which you want to import the task schedule settings.
- Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

```
Example of importing schedule settings from the configuration file /home/test/on_demand_schedule.ini into the task with ID=2
```

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

How to modify task schedule settings using command line options:

```
kesl-control --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `<setting name>=<setting value>` is the name and value of one task schedule setting.

Example of configuring a task to run every 10 hours

```
RuleType=Hourly
RunMissedStartRules=No
StartTime=2021/May/30 23:05:00;10
RandomInterval=0
```

Example of configuring a task to run every 10 minutes

```
RuleType=Minutely
RunMissedStartRules=No
StartTime=23:10:00;10
RandomInterval=0
```

Example of configuring a task to run on the 15th of each month

```
RuleType=Monthly
RunMissedStartRules=No
StartTime=23:25:00;15
RandomInterval=0
```

Example of configuring a task to run every Tuesday

```
RuleType=Weekly
StartTime=18:01:30;Tue
RandomInterval=99
RunMissedStartRules=No
```

Example of configuring a task to run every 11 days

```
RuleType=Daily
RunMissedStartRules=No
StartTime=23:15:00;11
RandomInterval=0
```

Managing general application settings

General application settings define the operation of the application as a whole and the operation of individual functions. Using general settings, you can:

- Configure the use of Kaspersky Security Network and the light version of anti-malware databases in the application.
- Configure the use of a proxy server in the application.
- Select the file operation interception mode (block/do not block files during a scan).
- Configure exclusions from the mount points scan (global exclusions).
- Configure exclusions from the process memory scan.

- Enable or disable Container Monitoring in real time.
- Enable or disable the detection of legitimate applications that intruders can use to compromise devices or data.
- Enable or disable integration with Kaspersky Managed Detection and Response.
- Configure the use of event logs.
- Configure a limit on CPU resource usage by scan tasks (of the ODS type).
- Limit the number of user scan tasks that a non-privileged user can start simultaneously.

You can manage general application settings using special management commands in the following ways:

- Using a configuration file. This method allows changing all general settings at the same time. You can get a configuration file to edit using the general settings output command.
- Using command line options in the <setting name>=<setting value> format. This method allows changing individual settings. You can get current values of settings using the general settings output command.

How to output the current values of the general application settings

You can output the current values of general application settings to the console or to a configuration file. You can then use this file to edit the settings.

```
Output the current values of the general settings of the application to the console

kesl-control --get-app-settings [--json]
```

Where `--json` is specified to output the settings in JSON format. If the `--json` option is not specified, the settings are output in the INI format.

```
Output the current values of the general settings of the application to a configuration file

kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Where `--file <path to configuration file>` is the path to the configuration file to which you want to output the general settings of the application. If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, the configuration file will not be created.

```
Example of writing general application settings to the kesl_config.ini file in the current directory

kesl-control --get-app-settings --file kesl_config.ini
```

How to edit task settings using a configuration file:

1. Output the general application settings to a configuration file using the `kesl-control --get-app-settings` command.
2. Open the resulting configuration file, edit the settings as necessary, and save your changes.
3. Run the following command:

   ```
   kesl-control --set-app-settings --file <path to configuration file> [--json]
   ```

where:

- `--file <path to configuration file>` is the full path to the configuration file with general application settings. If you delete any parameter in the configuration file, the default value for that parameter will be displayed after the command is executed.

- Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

All the values of the general settings defined in the file will be imported into the application.

```
Example of importing general settings into the application from the /home/test/kesl_config.ini configuration file

kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

How to change general settings using command line options

```
Change general settings using command line options

kesl-control --set-app-settings <setting name>=<setting value> [<setting name >=<setting value>]
```

Where `<setting name>=<setting value>` is the name and value of a general application setting.

The values of the specified general settings will be changed.

```
Example of setting a low level of detail for the trace file

kesl-control --set-app-settings TraceLevel=NotDetailed
```

```
Example of adding a mount point exclusion from file operation interception

kesl-control --set-app-settings ExcludedMountPoint.item_0000="/data"
```

Using filters to limit results of queries

A filter allows you to limit the query results when executing application management commands. Filter conditions are specified using one or more *logical expressions*, which are combined using the logical operator `and`. Filter conditions must be enclosed in quotation marks:

You can use a filter for the following purposes:

Display information about certain current events of the application

```
kesl-control -W --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Display information about certain application events in the event log

```
kesl-control -E --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Display information about certain objects in Backup

```
kesl-control -B --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator> '<value>']"
```

Delete certain objects from Backup

```
kesl-control -B --mass-remove --query "<field> <comparison operator> '<value>'[ and <field> <comparison operator>
'<value>']"
```

Where:

- `<field>` is the name of the field for the database.
- `<comparison operator>` is one of the following comparison operations:
  - > is "greater than"
  - < is "less than"
  - `like` matches the specified value When specifying a value, you can use % masks: for example, the logical expression `"FileName like '%etc%'"` sets the limitation "contains the text "etc" in the FileName field"

    > The `like` comparison operation works only with fields that are stored in the database as text. The `like` operation is not suitable for fields with dates, times, numbers, or other data types other than text.

  - == is "equal to"
  - `!=` is "not equal to"
  - >= is "greater than or equal to"
  - <= is "less than or equal to"

- <value> is the value of the field. The value must be enclosed in single quotation marks (').

  You can specify a date value as UNIX™ time (the number of seconds that have elapsed since 00:00:00 (UTC), January 1, 1970) or in YYYY-MM-DD hh:mm:ss format. The user specifies the date and time in the user's local time zone, and the application displays them in the same time zone.

Example output of information about events that contain the text "etc" in the FileName field

```
kesl-control -E --query "FileName like '%etc%'"
```

Example output of information about events with the ThreatDetected type

```
kesl-control -E --query "EventType == 'ThreatDetected'"
```

Example output of information about events with the ThreatDetected type, created by tasks of the ODS type

```
kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"
```

Example output of information about the events generated after the date specified in the UNIX time stamp system (the number of seconds that have elapsed since 00:00:00 (UTC), 1 January 1970)

```
kesl-control -E --query "Date > '1583425000'"
```

Example output of information about the events generated after the date specified in YYYY-MM-DD hh:mm:ss format

```
kesl-control -E --query "Date > '2022-12-22 18:52:45'"
```

Example output of information about files in the Backup storage that have the High severity level

```
kesl-control -B --query "DangerLevel == 'High'"
```

Exporting and importing application settings

Kaspersky Endpoint Security allows you to export and import all application settings for troubleshooting, verifying settings, or simplifying the application's configuration on other user devices.

Grant access to the configuration file only to trusted users. Before importing settings into the application, verify the paths to directories, configuration files, executable files, and the quarantine. Do not import configuration files from untrusted sources. Compromising the configuration file could affect the security, integrity, or functionality of the infrastructure of your organization, as well as user data.

Export settings

When exporting settings, all application settings (including general Container Scan settings, network traffic scan settings, general application settings, and task settings) are saved in a configuration file. You can use this configuration file to then import settings into the application.

Export application settings

```
kesl-control --export-settings --file <configuration file path> [--json]
```

Where:

- `--file <configuration file path>` is the full path to the configuration file to which you want to save application settings.
- `--json` is specified to export the settings to the configuration file in JSON format. If the `--json` options is not specified, the settings will be exported to an INI file.

Import settings

1. Run the following command:

   ```
   kesl-control --import-settings --file <configuration file path> [--json]
   ```

   Where:

   - `--file <configuration file path>` is the full path to the configuration file from which you want to import application settings.
   - `--json` is specified to import the settings from the configuration file in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

2. Restart the application.

Special considerations and limitations involved in exporting and importing settings

- The application must be launched when settings are imported or exported.
- If Kaspersky Endpoint Security is used in Light Agent mode, the settings of the predefined task of the `Update` type cannot be exported or imported.
- If changing the settings is prohibited by policy, then importing the settings is not available.
- If you are importing settings exported from an older version of the application into a newer version, the settings that did not exist in the older version are set to default values.
- You cannot import settings from a newer version to an older version.
- Some policy and task settings cannot be imported from the application web plug-in versions 12.3 and 12.4 into version 12.5 of the application. The limitation applies to the following policy and task settings:
  - Protection scope and exclusion scope of File Threat Protection and Anti-Cryptor
  - Exclusions of processes from scanning for Behavior Analysis
  - Trusted devices for Device Control
  - Scan scope and exclusion scope of System Integrity Monitoring

- Web Control rules
- Proxy server settings
- Exclusion from process memory scan
- Global exclusions (mount points excluded from scanning)
- Scan scopes of *ODS, ContainerScan*, *InventoryScan*, *ODFIM* tasks.

- After importing settings, the following is turned off: Kaspersky Security Network (`UseKSN=No`), cloud mode (`CloudMode=No`), and MDR integration (`UseMDR=No`). Manage the settings if you want to use this functionality.
- After application settings are imported, internal task IDs may change. It is recommended to use task names to manage tasks.
- When integrated with Kaspersky Endpoint Detection and Response Expert (cloud), all settings are exported, including settings received from Kaspersky Endpoint Detection and Response Expert (cloud):
  - Address and port of the telemetry server
  - Address and port of the response server
  - Connection timeout for the response servers
  - Response timeout for the response server
  - Connection timeout for the telemetry servers
  - Response timeout for the telemetry server
  - Client certificate of the telemetry server
  - Server certificate of the telemetry server
  - Client certificate of the response server
  - Server certificate of the response server

  When importing, the settings listed above are not imported to the device.

Managing the application via the graphical interface

Managing the application via the graphical interface requires the rights of the Administrator (admin) role.

If Kaspersky Endpoint Security is used in Light Agent mode, the graphical interface is not supported.

In **standard mode** of the application, you can use the graphical interface to:

- View information about device protection status.
- Configure application components.

  Selection tree

  - File Threat Protection.
  - Firewall Management.
  - Anti-Cryptor.
  - Removable Drives Scan.
  - Web Threat Protection.
  - Mail Threat Protection.
  - Device Control.
  - Network Threat Protection.
  - BadUSB Attack Prevention.
  - Behavior Detection.
  - Exploit Prevention.
  - Application Control.
  - Web Control.
  - System Integrity Monitoring.
- Scan files and directories, including sending files to Sandbox for scanning.
- Start an update and roll back database updates.
- Enable or disable Kaspersky Security Network for the application.
- Request and obtain temporary access to a blocked device from the administrator of the organization's local network.
- Manage application license keys and view information about currently used licenses and keys.
- View information about objects placed in Backup.
- View application reports.
- Create application trace files.

Application icon in the notification area

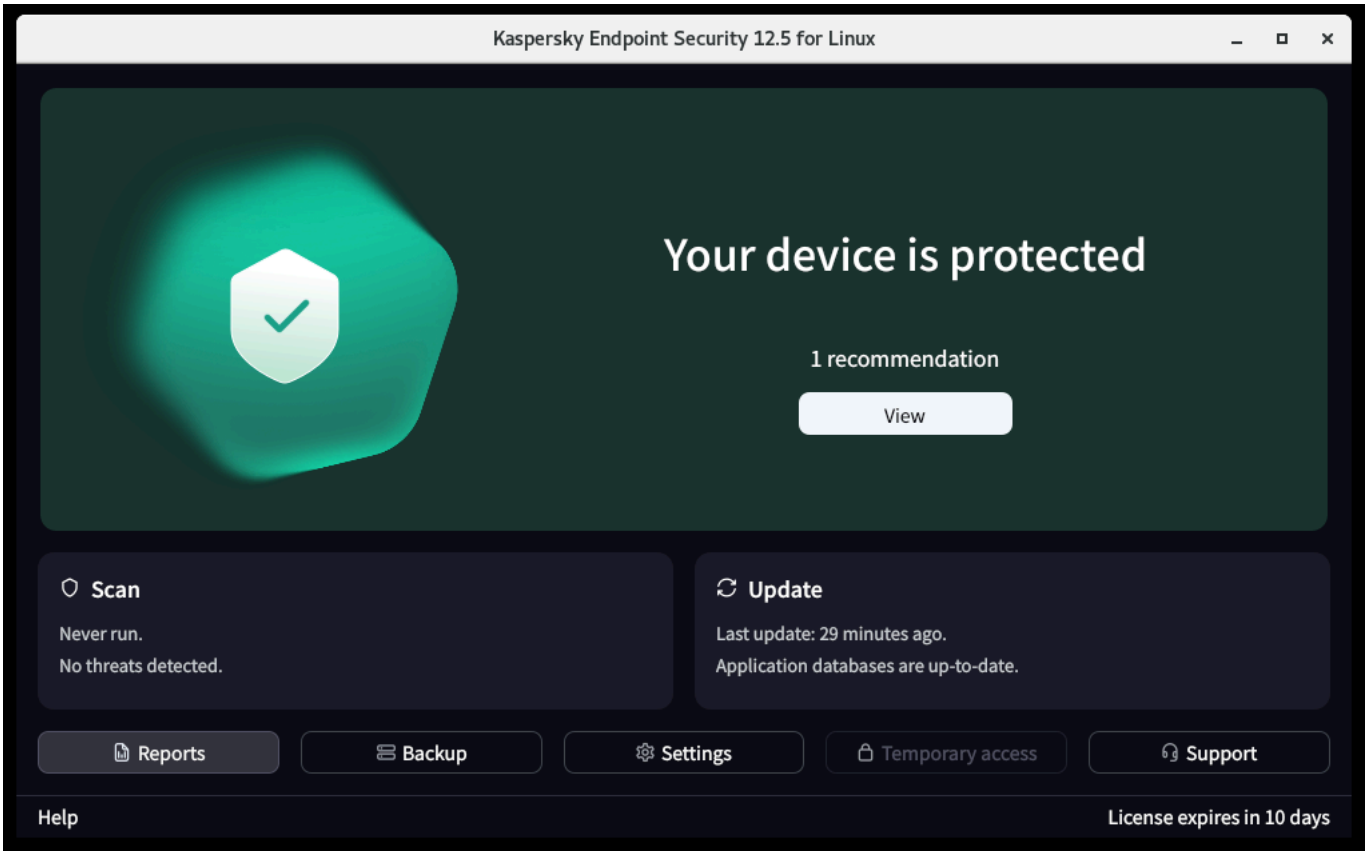
The Kaspersky Endpoint Security icon in the tray provides access to the context menu and the main window of the graphical interface of the application.

> In some operating systems, the default application icon may be missing after installing the application graphical interface package.

The context menu of the application icon contains the following items:

- **Kaspersky Endpoint Security 12.5 for Linux**. Opens the main window of the application's graphical interface.
- **Exit**. Exits the graphical interface.

The main window of the application graphical interface



Main application window

Protection status	Information about device protection status. Displayed in the upper part of the main window. You can click the **View** button to open the **Protection Center** window. This window displays recommendations on the actions to be performed to fix protection problems (if any).
Scan	Information about the Malware Scan task status and the number of detected threats. You can click this section to open the **Scan** window. In this window, you can start and stop *Malware Scan*, *Critical Areas Scan*, and *Container Scan* tasks and view reports for these tasks.

Update	Information about the status of the database update task. You can click this section to open the **Update** window. In this window, you can start *Update* and *Rollback* tasks and view reports for these tasks.
Reporting	Viewing reports and statistics for components and tasks.
Backup	Viewing object details in Backup. What to do if the button is inactive
Settings	Enabling or disabling application components, configuring Kaspersky Security Network. What to do if the button is inactive
Temporary access	Requesting and obtaining temporary access to a blocked device.
Support	Information about the application: current version of Kaspersky Endpoint Security, database release date, key, and other information. You can also visit Kaspersky resources to get useful information or contact Technical Support.
License term	Remaining license term You can click this area to open the **Licenses** window. In this window, you can view detailed information about your license or visit the Kaspersky website to purchase a new license.

Protection status monitoring

Protection status of Kaspersky Security Center client devices

You can get information about the protection status of a device in Kaspersky Security Center using the statuses of client devices. For Kaspersky Security Center, a client device is a device on which Kaspersky Security Center Network Agent is installed.

The status of the client device status can change to *Critical* or *Warning* in accordance with the rules configured in Kaspersky Security Center. For example, the status may change if a protection application is not installed on the device, a virus scan has not been performed for a long time, the application databases are out of date, the license has expired, or if Kaspersky Security Center has received the device status from a managed application.

For more details on the reasons for changing statuses and configuring conditions for assigning statuses, refer to the Kaspersky Security Center Help.

How to check the protection status of a device in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.

4. This opens the properties window of the managed device; in that window, on the **General** tab, select the **Protection** section.

The **Protection** section displays the following information about the device:

- **Visible in the network** is the visibility of the selected device in the network: *Yes* or *No*.
- **Device status** is the status of the client device generated based on the protection status criteria set by the administrator for the selected device and the device activity in the network: *OK*, *Critical*, or *Warning*.
- **Status description** represents the reasons for changing the status of the device to *Critical* or *Warning*.
- **Protection status** represents the current status of File Threat Protection on the selected device, such as *Running*, *Stopped*, or *Paused*.
- **Last full check** represents date and time when the last full scan task was completed on the selected device.
- **Virus detected** represents the total count of malicious objects detected on the selected device (detected threat counter) since Kaspersky Endpoint Security was installed.
- **Objects that failed disinfection** represents a number of infected objects that Kaspersky Endpoint Security was unable to disinfect.

How to check the protection status of a device in the Administration Console

1. In the Administration Console tree, in the **Managed devices** folder, select the administration group containing the necessary device.
2. In the workspace, select the **Devices** tab.
3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.
4. In the window that opens with the properties for the managed device, select the **Protection** section.

The **Protection** section displays the following information about the device:

- **Device status**: status of the client device generated based on the criteria set by the administrator for the protection status of the selected device and the device activity in the network.
- **All problems**: complete list of problems detected by the managed applications installed on the selected device. Each problem has a status that the application prompts to assign to the device.
- **Real-Time Protection status**: current status of File Threat Protection on the selected device, such as *Running* or *Stopped*. When the protection status changes, the new status is displayed in the device properties window only after the device is synchronized with the Administration Server.
- **Last on-demand scan**: date and time when the last malware scan was performed on the selected device.
- **Total threats detected**: total number of threats detected on the selected device since the installation of the application (first scan) or since the last reset of the threat counter.

  To reset the counter, click the **Reset** button.
- **Active threats**: the number of unprocessed files on the selected device.

For more details on client device statuses, refer to the Kaspersky Security Center Help.

General information about the operation of the application on the device

How to view general information about the application in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. In the list of applications installed on the device, click Kaspersky Endpoint Security.

   The application properties window opens.

6. View the general information about the application on the **General** tab in the **Information** section:

   - **Name** is the name of the application.
   - **Version** is the version number of the application.
   - **Installed** is the date and time when the application was installed on the device.
   - **Last software update**: date and time when Kaspersky Endpoint Security software modules were last updated.
   - **Last synchronization** is the date and time of the last connection of the device to the Kaspersky Security Center Administration Server.
   - **Current status** is the state of the application on the device, for example, *Running* or *Stopped*.
   - The **Installed updates** block contains information about installed versions of application updates.
   - Under **Application databases**, you can find information about the date and time of the application database update release and the date and time of the last update.

7. View information about functional components of the application on the **General** tab in the **Components** section. The status (for example, *Stopped, Suspended, Not Installed*) and version of each component is displayed.

8. View the list of application events on the device on the **Events** tab.

How to view general information about the application in the Administration Console

1. In the Kaspersky Security Center Administration Console tree, in the **Managed devices** folder, select the administration group containing the required device.

2. In the workspace, select the **Devices** tab.

3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.

4. In the displayed window with the properties of the managed device, select the **Applications** section.

   The right part of the window displays a list of Kaspersky applications installed on the device.

5. Select Kaspersky Endpoint Security and double-click it to open the application properties window. Alternatively, you can use the **Properties** button in the lower part of the window.

   The application properties window opens.

6. View general information about the application line in the **General** section.

   - **Version number**: the version number of the application.
   - **Installed** is the date and time when the application was installed on the device.
   - **Current status** is the status of the application (kesl service). The application can have a status such as *Running* or *Paused*.
   - **Last software update**: date and time when Kaspersky Endpoint Security software modules were last updated.
   - **Installed updates** is the information about installed versions of application updates.
   - **Application databases** is the date and time when the application database update was released.

7. View information about the functional components of the application in the **Components** section. The status (for example, *Stopped, Suspended, Not Installed*) and version of each component is displayed.

How to view general information about the application on the command line

```
Run the following command:

kesl-control --app-info [--json] [--check-permissions]
```

Where:

`--json`: output data in JSON format.

`--check-permissions` displays paths to application directories with incorrectly configured permissions.

As a result of the command execution, the following information will be displayed in the console:

- **Name**. Application name.
- **Version**. Current application version.
- **Policy**. Information about whether a Kaspersky Security Center policy is applied on the device.
- Extended information about the policy applied on the device:
  - Policy name.
  - The date and time when the policy was last applied or updated on the device.

- Kaspersky Security Center administration group to which the device belongs.
- List of policy profiles applied on the device (if any).

> Extended policy information is displayed if the **Application is allowed to retrieve policy's extended data on device** setting of the Network Agent that is installed on the device allows retrieving of extended policy data from Kaspersky Endpoint Security. This setting is disabled by default. For details about Network Agent settings, please refer to the Kaspersky Security Center Help.

- Information about the license under which the application is used:
  - **Application license information**. Application license information or application license key status.
  - **Kaspersky Endpoint Security license expiration date**. Application license expiration date and time (UTC).
- License information for the Endpoint Detection and Response Optimum component and components for integration with Kaspersky solutions. The fields are displayed if the following components are activated on the protected device:
  - **EDR Optimum license information**. Information about the license under which the Endpoint Detection and Response Optimum component is activated, or the status of the EDR Optimum license key.
  - **EDR Optimum license expiration date.** License expiration date and time (UTC).
  - **KUMA license information**. Information about the license under which the Kaspersky Unified Monitoring and Analysis Platform functionality is being used, or the status of the KUMA license key.
  - **KUMA license expiration date**. License expiration date and time (UTC).
  - **MDR license information**. Information about the license under which the Managed Detection and Response component is activated, or the status of the MDR license key.
  - **MDR license expiration date**. License expiration date and time (UTC).
  - **EDR Expert (on-premises) license information**. Information about the license that the Endpoint Detection and Response Expert (on-premises) component is activated with, or the EDR Expert (on-premises) license key status.
  - **License expiration date for EDR Expert (on-premises)**. License expiration date and time (UTC).
  - **EDR Expert (cloud) license information**. Information about the license that the Endpoint Detection and Response Expert (on-premise) component is activated with, or the EDR Expert (cloud) license key status.
  - **License expiration date for EDR Expert (cloud)**. License expiration date and time (UTC).
- **Subscription status**. Status of the subscription. This field is displayed if the application is started under a subscription.
- **MDR BLOB file status**. Status of the MDR BLOB file for integration with Kaspersky Managed Detection and Response.
- **Expiration date of license from MDR BLOB file**. Kaspersky Managed Detection and Response license expiration date and time (UTC). This field is displayed if a BLOB configuration file has been loaded for the Kaspersky Managed Detection and Response integration.

- **Backup state**. Information about the status of Backup.
- **Backup usage**. Backup size.
- **Last run date of the Scan_My_Computer task**. Time of the last Malware Scan task.
- **Last release date of databases**. Date and time the application databases were last released.
- **Application databases loaded**. Information about whether the application databases were downloaded.
- **Updatable kernel module status**. Information about the status of the updatable kernel module.
- **Kaspersky Security Network usage**. Information about using Kaspersky Security Network: `Extended KSN mode`, `Basic KSN mode` or `Disabled`.
- **Light Agent mode**. Information about the application being used in Light Agent mode. If the application is being used in Standard mode or in Endpoint Detection and Response Agent mode, this line is not displayed.
- **Endpoint Detection and Response Agent mode**. Information about the application being used in EDR Agent mode. If the application is being used in Basic mode or Light Agent mode, this line is not displayed.
- **Kaspersky Security Network infrastructure**. Information about the infrastructure solution used to work with Kaspersky reputation databases: `Kaspersky Security Network` or `Kaspersky Private Security Network`.
- **Kaspersky Managed Detection and Response Integration**. Kaspersky Managed Detection and Response integration status.
- **Kaspersky Endpoint Detection and Response Optimum Integration**. Status of integration with Kaspersky Endpoint Detection and Response Optimum.
- **File Threat Protection**. Real-time File Threat Protection status.
- **Container monitoring**. Real-time Container Scan status.
- **System Integrity Monitoring**. System Integrity Monitoring component status.
- **Firewall Management**. Firewall Management component status.
- **Anti-Cryptor**. Anti-Cryptor component status.
- **Web Threat Protection**. Web Threat Protection component status.
- **Device Control**. Device Control component status.
- **Removable Drives Scan**. Removable Drives Scan component status.
- **BadUSB Attack Prevention**. BadUSB Attack Prevention component status.
- **Network Threat Protection**. Network Threat Protection component status.
- **Behavior Detection**. Behavior Detection component status.
- **Application Control**. Application Control component status.

- **Web Control**. Web Control component status.
- **Kaspersky Endpoint Detection and Response Expert (on-premises) Integration**. Status of the integration with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA).
- **Kaspersky Endpoint Detection and Response Expert (cloud) integration**. Kaspersky Endpoint Detection and Response Expert (cloud) integration status.
- **Sandbox Integration**. Sandbox Integration status.
- **Kaspersky Unified Monitoring and Analysis Platform Integration**. Kaspersky Unified Monitoring and Analysis Platform Integration status.
- **Kaspersky Network Detection and Response (KATA) Integration** Kaspersky Network Detection and Response (KATA) integration status.
- **Mail Threat Protection**. Mail Threat Protection component status.
- **Post-update actions**. Application update actions and the actions to be performed by the user.
- **Application is unstable**. Information about dumping in case of application crash. This field is displayed if any files are found in the dump directory.
- **Application status**. Information about the Network Agent connection status and permissions for system directories:
  - *OK*. Network Agent is connected, permissions for system directories are configured correctly.
  - *Critical. No connection to the Network Agent*.
  - *Critical. Permissions for system directories are configured incorrectly*.
  - *Critical. No connection to the Network Agent. Permissions for system directories are configured incorrectly*.

How to view general information about the application in the graphical interface

1. Open the main window of the application graphical interface.
2. In the lower part of the main window, click the **Support** button.

   The **Support** window opens.
3. View general information about the device and the installed application:
   - Application version.
   - **License key** displays the active main license key added to the application, or a message saying that no key has been added. Clicking the link in this field opens the **Licenses** window, which displays detailed license information.
   - **Key status** displays information about the status of the active main license key, or a message saying that no key has been added.
   - **Database release date** – status and release date of the application databases.

- **Operating system** – information about the operating system of the device.
- **Application management** – Information about whether the device is managed by a policy.

If the **Application is allowed to retrieve policy's extended data on device** option is enabled in the Network Agent policy, the window also displays the following information about the policy that is applied on the device with the application installed.

- **Policy name** is the name of the policy that is applied to the device on which application is installed.
- **Date applied** – the date and time when the policy was last applied or updated on the device with the installed application.
- **Administration group** is the name of the administration group that includes the device on which the application is installed, that is managed by a policy.
- **Active policy profiles** is a list of active policy profiles applied on the device (if any).

Application statistics

You can view statistics for the most frequently scanned files and started processes.

You can configure how the application calculates and displays statistics in the kesl.ini configuration file in the `[ScannerImpactStats]` section.

How to view scan statistics in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.
4. This opens a managed device properties window; in that window, go to the **Applications** tab.
5. In the list of applications installed on the device, click Kaspersky Endpoint Security.
6. In the application properties window that opens, on the **Application settings** tab, select **Statistics** → **Scan statistics**.

7. View application statistics in the **Scan statistics** window:

   - The **Most frequently scanned applications (File Threat Protection)** block displays the paths to the applications that the File Threat Protection component scans most frequently, and the number of times the component accesses these applications. Files are displayed in descending order of the number of times they are accessed.

   - Under **Most frequently started processes**, you can find paths to the processes that Kaspersky Endpoint Security detects most often and the number of such process starts. Paths to processes are displayed in descending order of the number of process starts.

   You can click **Export** buttons in the upper part of each area to export the corresponding statistics to a text file.

How to view scan statistics in the Administration Console

1. In the Kaspersky Security Center Administration Console tree, in the **Managed devices** folder, select the administration group containing the required device.

2. In the workspace, select the **Devices** tab.

3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.

4. In the displayed window with the properties of the managed device, select the **Applications** section.

   The right part of the window displays a list of Kaspersky applications installed on the device.

5. Select Kaspersky Endpoint Security and double-click it to open the application properties window. Alternatively, you can use the **Properties** button in the lower part of the window.

6. In the window that opens, select **Statistics** → **Scan statistics**.

7. View application statistics:

   - The **Most frequently scanned applications (File Threat Protection)** block displays the paths to the applications that the File Threat Protection component scans most frequently, and the number of times the component accesses these applications. Files are displayed in descending order of the number of times they are accessed.

   - Under **Most frequently started processes**, you can find paths to the processes that Kaspersky Endpoint Security detects most often and the number of such process starts. Paths to processes are displayed in descending order of the number of process starts.

   You can click **Export** buttons under each area to export the corresponding statistics to a text file.

How to view scan statistics on the command line

```
Run the following command:

kesl-control [-S] --get-statistic [--files] [--processes]
```

Where:

- `--files`: statistics of files most frequently scanned by the File Threat Protection component, and the number of times the component accesses these files.
- `--processes`: statistics of process starts most frequently detected by Kaspersky Endpoint Security, and the number of such starts.

  Excluding processes from scanning by the Behavior Detection component does not remove these processes from statistics, but it improves the performance of the Kaspersky Endpoint Security application.

If you do not specify any options, the application displays three lists: statistics on the most frequently scanned files, statistics on the most frequently started processes, and the list of mount points found on the device.

On CentOS 5.2, 5.4, 6.4 and 6.6, statistics of frequently scanned files is not collected.

Discovered mount points

You can view the list of mount points found on the device. The list displays information indicating whether the mount point has been added to scan exclusions.

How to view the list of mount points in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. In the list of applications installed on the device, click Kaspersky Endpoint Security.

6. In the application properties window that opens, on the **Application settings** tab, select **Statistics** → **Mount points**.

   The **Mount points** window opens.

7. View information about mount points in the table:

   - **Mount point path** is the path to the mount point detected on the device.
   - **Namespace** indicates whether the mount point is found in a namespace.
   - **Excluded** indicates whether the mount point has been added to scan exclusions.

Mount point paths are sorted as follows:

- Static, system, service and other mount points
- Mounted snap packages and mount points in their namespaces
- Mount points created by the Docker container management system

By clicking the **Export** button in the upper part of the window above the list, you can export the list of mount points to a text file. The file contains a list of mount point paths, as well as the **[Namespace]** and **[Excluded]** tags.

How to view the list of mount points in the Administration Console

1. In the Kaspersky Security Center Administration Console tree, in the **Managed devices** folder, select the administration group containing the required device.
2. In the workspace, select the **Devices** tab.
3. In the list of managed devices, select the required device and double-click it to open the **Properties: <Task name>** window.
4. In the displayed window with the properties of the managed device, select the **Applications** section.

   The right part of the window displays a list of Kaspersky applications installed on the device.
5. Select Kaspersky Endpoint Security and double-click it to open the application properties window. Alternatively, you can use the **Properties** button in the lower part of the window.
6. This opens the application properties window; in that window, select the **Statistics** → **Mount points** section.
7. View information about mount points in the **List of mount points** table:

   - **Mount point path** is the path to the mount point detected on the device.
   - **Namespace** indicates whether the mount point is found in a namespace.
   - **Excluded** indicates whether the mount point has been added to scan exclusions.

   Mount point paths are sorted as follows:

   - Static, system, service and other mount points
   - Mounted snap packages and mount points in their namespaces
   - Mount points created by the Docker container management system

   By clicking the **Export** button below the list, you can export the list of mount points to a file in text format. The file contains a list of mount point paths, as well as the `[Namespace]` and `[Excluded]` tags.

How to view the list of mount points on the command line

```
Run the following command:

kesl-control [-S] --get-statistic --mountpoints
```

The output includes the following information:

- `[excluded]` indicates whether the mount point has been added to scan exclusions.
- `[namespace]`, indicating whether the mount point is found in a namespace.
- Path to the mount point found on the device.

Mount point paths are sorted as follows:

- Static, system, service and other mount points
- Mounted snap packages and mount points in their namespaces
- Mount points created by the Docker container management system

List of functionality and technologies

On the command line, you can view the list of application functionality with status information (used or not used) and the Linux technologies that these application functionality is implemented with.

```
View the list of functionality and technologies

kesl-control --supported-tech-info
```

As a result of the command execution, the following information will be displayed in the console:

Interception of file operations:

Status: In use or Not in use

Technologies: fanotify, File Threat Protection kernel module, updatable kernel module.

Interception of process start:

Status: In use or Not in use

Technologies: eBPF, kprobe, netlink, undefined, updatable kernel module.

Scanning network traffic:

Status: In use or Not in use

Technologies: eBPF, iptables, undefined.

iptables utility:

Status: In use or Not in use

Technologies: ipv6, undefined, timeout, support for multiple labels in rules.

Network isolation:

Status: In use or Not in use

Technologies: eBPF, iptables, undefined.

Exploit Prevention:

Status: In use or Not in use

Technologies: undefined, updatable kernel module.

Real-Time Protection statuses

The Real-Time Computer Protection status determines the status of the File Threat Protection component. File Threat Protection provides a minimum level of security to the computer. The component is started together with Kaspersky Endpoint Security and scans files in real time.

Real-Time Protection statuses

Status in Kaspersky Security Center	Status on the command line	Description
Running	Started	The File Threat Protection task is started and running.
Starting	Starting or Resuming	Attempt to run the File Threat Protection task. Wait for the task to start.
Stopped	Stopped or Stopping	The File Threat Protection task was stopped manually. Run the task in Kaspersky Security Center or locally on the computer. If the application is installed in Light Agent mode, the device gets this status when there is no connectivity with the SVM.
Paused	Pausing or Suspended	The File Threat Protection task was paused manually. Run the task in Kaspersky Security Center or locally on the computer.
Not set		The application is installed in EDR Agent mode. The File Threat Protection component operates in Inform mode.
Unknown		Unknown error.

How to find out the Real-Time Computer Protection status

You can find out the status of Real-Time Computer Protection in a Kaspersky Security Center console in the list of managed devices or locally on your computer.

How to find out the Real-Time Computer Protection in the Web Console

In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

The current protection status is displayed in the list of devices, in the **Real-time protection status** column. If the **Real-time protection status** is column missing, manage column settings (⚙).

How to find out the Real-Time Computer Protection on the command line

```
Run the following command:

kesl-control --get-task-state 1
```

As a result, Kaspersky Endpoint Security will display information about the operation of File Threat Protection in the following format:

Name: File_Threat_Protection	
ID	: 1
Type	: OAS
State	: <protection status>

What to do if the Real-Time Computer Protection status is not Running

1. Make sure File Threat Protection is enabled in the policy properties.
2. Make sure that the application is activated.
3. Try running the File Threat Protection task:

   How to run the File Threat Protection task in the Web Console

   1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

      The list of managed devices opens.
   2. Find your device in the list and click on its name.
   3. This opens a managed device properties window; in that window, go to the **Tasks** tab.

      This opens a list of all tasks on the device.
   4. Select the **File Threat Protection** task and click the **Run** button.

   How to run the File Threat Protection task in the command line

   ```
   Run the following command:

   kesl-control --start-task 1
   ```

Events and reports

While the application is running, various *events* occur. The events may be informational or may contain important data. For example, the application can use an event to inform about a successful application database update, or about an error of application components that needs to be fixed.

Kaspersky Endpoint Security saves information about application events to the following logs:

- The application event log. By default, the application stores event information in event log database files located in the /var/opt/kaspersky/kesl/private/storage directory. You can configure the application event log in the command line.
- Operating system log (syslog). The operating system log is not used by default. You can enable saving events to this log.

Access to the application event log and operating system log requires root privileges.

If Kaspersky Endpoint Security is managed by Kaspersky Security Center, information about events may be transmitted to the Kaspersky Security Center Administration Server. Aggregation rules apply to certain events. If a large number of same-type events are created within a short period of time while the application is running, the application will switch to event aggregation mode and send to Kaspersky Security Center one aggregated event with a description of the events settings. Different aggregation rules may be used for different events. For more information about events, refer to the Kaspersky Security Center Help.

You can receive information about application events in the following ways:

- In the Administration Console and in the Web Console
- In the command line
- When using the application's graphical user interface – in pop-up notifications if displaying notifications is enabled in the policy properties or in the application's general settings

The application can generate various types of *reports* on the events that occur while the application is running. Reports contain information about the operation of each Kaspersky Endpoint Security component, the results of each task, and the overall operation of the application.

You can view reports in the following ways:

- Kaspersky Security Center reports are available in the Administration Console and in the Web Console. You can use these to get information about infected files or usage of keys and application databases, among other things. For detailed information on working with Kaspersky Security Center reports, please refer to the Kaspersky Security Center Help.
- The graphical user interface of Kaspersky Endpoint Security displays reports of the application, its components and tasks.

Contents of reports and events

Events and reports may contain the following personal data:

- User name and user ID of operating system users
- Paths to user files
- IP addresses of remote devices that are scanned by the Anti-Cryptor component
- IP addresses of senders and receivers of network packets scanned by the Firewall Management component

- Web addresses of the update sources
- General application settings values
- Names and settings of command line tasks
- Detected malicious, phishing, adware web addresses, and web addresses containing legitimate applications that intruders can use to compromise devices or data
- Names of the containers and images
- Paths to the containers and images
- Names and IDs of the devices
- Names of application categories
- Web addresses of the repositories
- File names, paths, and hashes of executable files of applications

Rules of escaping characters in file paths

Some events may contain file paths. For output, the file path is treated as a UTF-8 string. If any of the bytes in the path does not comply with the UTF-8 encoding rules, is it replaced with the `?` character. Any four-byte sequence that encodes a character code outside the Unicode range (greater than 0x10FFFF) is also replaced with the `?` character. Special characters are escaped (replaced) in a certain way.

The following rules apply for escaping characters in file paths inside events in the output of `kesl-control -E --query`:

- '\a', '\b', '\t', '\n', '\v', '\f', '\r' characters are replaced by two characters as follows:

  '\a' -> "\\a"

  '\b' -> "\\b"

  '\t' -> "\\t"

  '\n' -> "\\n"

  '\v' -> "\\v"

  '\f' -> "\\f"

  '\r' -> "\\r"

- All other special characters are output without modification.

The following rules apply for escaping characters in file paths inside events in the output of `kesl-control -E --query --json`:

- In accordance with the JSON format, the '\b', '\f', '\n', '\r', '\t', '"', '\\' characters are escaped as follows:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

"" -> "\\\ ""

'\\' -> "\\\\"

- All other special characters are escaped in accordance with the general JSON rules for escaping special characters ('\a' -> '\u0007').

Rules for escaping characters in file paths in events when sending to syslog:

- In accordance with the JSON format, the '\b', '\f', '\n', '\r', '\t', "", '\\' characters are escaped as follows:

  '\b' -> "\\b"

  '\f' -> "\\f"

  '\n' -> "\\n"

  '\r' -> "\\r"

  '\t' -> "\\t"

  "" -> "\\\ ""

  '\\' -> "\\\\"

- All other special characters are escaped in accordance with the general JSON rules for escaping special characters ('\a' -> '\u0007').

The first backslash in the sequence when describing rules is the escape character.

Examples:
`'\a'` is one character (a control character).

`'\\a'` is two characters (backslash + the "a" character).

`'\\'` is one character (backslash), `'\\\\'` is two characters (backslash + backslash).

Configuring event logging to the operating system log

Events that occur during the operation of Kaspersky Endpoint Security can be recorded in the operating system log (syslog). You can enable or disable the recording of events in this log using the Web Console, Administration Console, or the command line.

By default, logging of events in the operating system log is disabled.

If Kaspersky Endpoint Security is running in standard mode or EDR Agent mode and is managed by a policy in Kaspersky Security Center, information about the addition and removal of license keys and license expiration is logged in the operating system log by default. You can select the events that you want to be recorded in the operating system log in the properties of the policy that is applied to the application.

How to configure logging of events to syslog in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security for Linux policy.

   The policy properties window opens.

3. Go to the **Application settings** tab.

4. Select **General Settings** → **Event settings**.

   Event types are displayed grouped by severity.

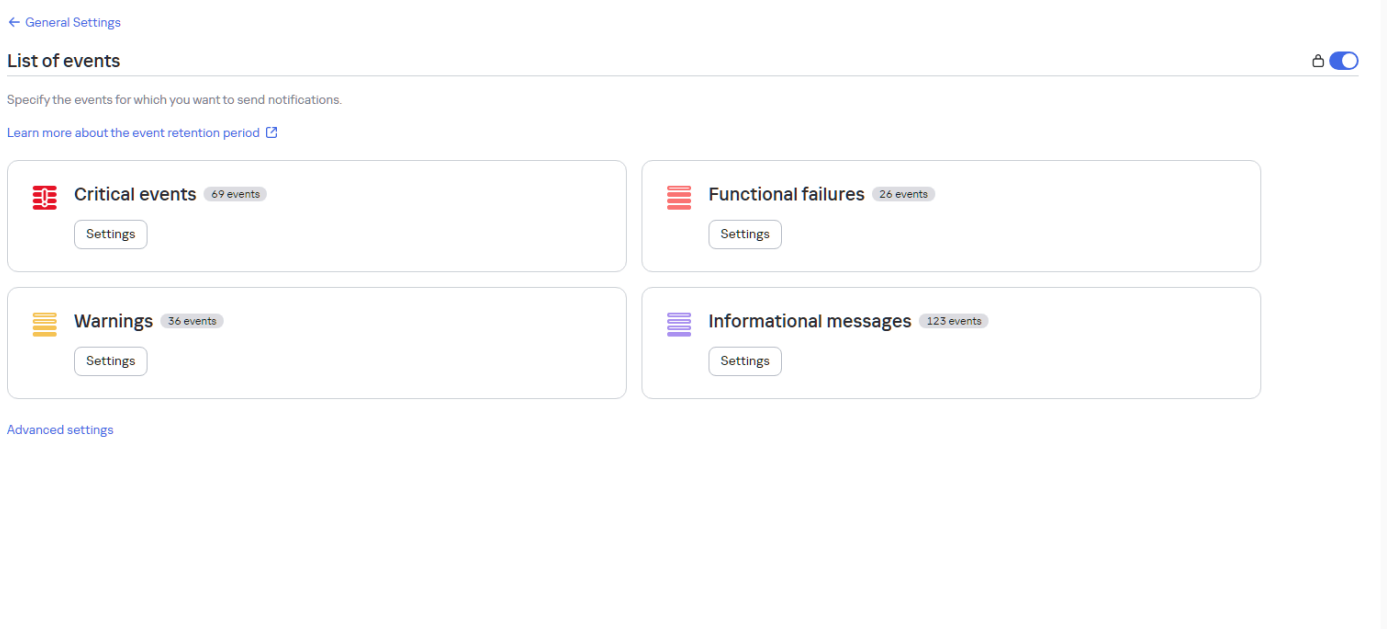
5. Click the **Settings** button in the block with the name of the severity level corresponding to the event for which you want to configure logging to the operating system log.

   This opens a window with a list of all events of the selected severity level. You can independently enable or disable logging to the operating system log for each event.

6. In the **Events** column, click the name of the event for which you want to configure logging in the operating system log.

7. Go to the **Notifications** tab.

8. Select or clear the **Save in the operating system event log** check box.



Event notification settings

How to configure logging of events to syslog in the Administration Console

1. In the tree of the Kaspersky Security Center Administration Console, in the **Managed devices** folder, open the folder with the name of the administration group that includes the required devices.

2. In the workspace, select the **Policies** tab.

3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.

4. Go to the **General settings** → **Interface** section.

5. Under **Notifications**, click **Configure**.

   The **Notification settings** window opens.

6. Use the check boxes to select the events that the application records in the operating system log.

You can also select all events of a certain severity level:

- *Critical events* pose a serious threat to the device's security (detection of malicious objects, vulnerabilities, problems with the operation of the application). Critical events require your immediate attention. We recommend not to disable critical event notifications.

- *Functional failures* occur when the application fails (processing error, task misconfiguration). Such events do not pose a direct threat to the security of the device, but they require your actions for the application to work correctly.

- *Warnings* do not require your immediate action, but may indicate a potential future threat to the security of the device.

- *Informational messages* correspond to events of an informational nature.

How to configure logging of events to syslog on the command line

You can enable or disable saving events to the operating system log in the command line via the `UseSyslog` option in the general application settings.

You can edit the option via command line switches or a configuration file that contains all general application settings.

```
Enable or disable logging of events to syslog

kesl-control --set-app-settings UseSyslog=<Yes|No>
```

Where:

- `Yes`: enable saving of all events to syslog.

- `No` (default): disable saving events to syslog.

Configuring application event log settings

By default, information about events is saved to the application event log located on the device.

The event log database contains the following files:

- Several files with events. The number of files depends on the current number of events in the event log and on the maximum number of events that the application is configured to store (the `MaxEventsNumber` setting).

  The name of the file with events includes its serial number (for example, events.db.0001). When a file fills up, a new file is created. If the maximum number of events in all event files not counting the earliest file reaches the `MaxEventsNumber` value, the earliest file is deleted. This means that the application may store more events than indicated in the setting.

- The main file of the database for managing event files that stores information about the event log files. This file cannot be deleted.

You can manage the following application event log options on the command line via the general application settings:

- Change the path to the application event log database using the `EventsStoragePath` setting. Default value: /var/opt/kaspersky/kesl/private/storage/events.db.
- Specify the maximum number of events to be stored by the application via the `MaxEventsNumber` option. Default value: 500000.

You can view the current settings in the general application settings on the command line or in the configuration file.

```
Output the current values of the general settings of the application to the console
kesl-control --get-app-settings [--json]
```

Where `--json` is specified to output the settings in JSON format.

```
Output the current values of the general settings of the application to a configuration file
kesl-control --get-app-settings --file <path to configuration file> [--json]
```

Where `--file <path to configuration file>` is the path to the configuration file to which you want to output the general settings of the application. If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, the configuration file will not be created.

You can change the values of the settings with the help of command line switches or a configuration file that contains all general application settings.

```
Modifying event settings using command line options
kesl-control --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Where <setting name>=<setting value> is the name and value of one of the settings.

```
Change event settings using the configuration file
kesl-control --set-app-settings --file <path to configuration file> [--json]
```

Where:

- `--file <path to configuration file>` is the full path to the configuration file with general application settings. If you delete any parameter in the configuration file, the default value for that parameter will be displayed after the command is executed.
- Specify the `--json` option if you are importing settings from a JSON configuration file. If the --json option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

All the values of the general settings defined in the file will be imported into the application.

Viewing application events

Viewing all events of the Kaspersky Endpoint Security application in Kaspersky Security Center

Events of the Kaspersky Endpoint Security application fall into the following types by severity:

- *Critical events* pose a serious threat to the device's security (detection of malicious objects, vulnerabilities, problems with the operation of the application). Critical events require your immediate attention. We recommend not to disable critical event notifications.
- *Functional failures* occur when the application fails (processing error, task misconfiguration). Such events do not pose a direct threat to the security of the device, but they require your actions for the application to work correctly.
- *Warnings* do not require your immediate action, but may indicate a potential future threat to the security of the device.
- *Informational messages* correspond to events of an informational nature.

A list of all Kaspersky Endpoint Security events is displayed in the Web Console and in the Administration Console.

How to view the list of all events in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Go to the **Event configuration** tab.

   A list of all events is displayed, filtered by severity.
4. Use the menu on the left to view all events of other severity levels.

How to view the list of all events in the Administration Console

1. In the tree of the Kaspersky Security Center Administration Console, in the **Managed devices** folder, open the folder with the name of the administration group that includes the required devices.
2. In the workspace, select the **Policies** tab.
3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.
4. Go to the **General settings** → **Notification settings** section.
5. Under **Notifications**, click **Configure**.

   The **Notification settings** window opens.

You can configure event notifications. Notifications give you timely information about application events. You can configure the execution of a script upon receiving events from the application or upon receiving notifications about events by e-mail. For detailed information about using Kaspersky Security Center notifications, refer to the Kaspersky Security Center Help.

Viewing events in the graphical interface of the application

By default, in the graphical interface of the application, information about events is displayed in pop-up notifications.

How to configure pop-up notifications in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security for Linux policy.

   The policy properties window opens.
3. Go to the **Application settings** tab.
4. Select **General Settings** → **Event settings**.
5. Click the **Additional settings** link.

   The **Additional settings** window opens.
6. Select or clear the **Show pop-up notifications in the graphical user interface** check box. This check box is selected by default.
7. Save your changes.

How to configure pop-up notifications in the Administration Console

1. In the tree of the Kaspersky Security Center Administration Console, in the **Managed devices** folder, open the folder with the name of the administration group that includes the required devices.
2. In the workspace, select the **Policies** tab.
3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.
4. Go to the **General settings** → **Notification settings** section.
5. Select or clear the **Show pop-up notifications in the graphical user interface** check box. This check box is selected by default.

How to configure pop-up notifications on the command line

On the command line, you can enable or disable pop-up notifications in the graphical interface using the `ShowPopUpNotifications` setting in the General application settings.

You can change the value of the setting with the help of command line switches or a configuration file that contains all general application settings.

```
Enables displaying pop-up notifications in the graphical interface

kesl-control --set-app-settings ShowPopUpNotifications=<Yes|No>
```

Where:

- `Yes` (default value) – show pop-up notifications in the graphical user interface.
- `No` – do not show pop-up notifications in the graphical user interface.

Viewing current events of the Kaspersky Endpoint Security application on the command line

On the command line, you can output information about all current events in the application or events related to the specified task. You can use the filter to output certain current events, for example, events of a specified type.

```
Display in the console information about all current application events

kesl-control -W
```

The command returns the name of the event and additional information about the event.

```
Run the task and output information about current events associated with it to the console

kesl-control --start-task <task ID|name> -W
```

where `<<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task in the command line.

The command starts the task with the specified ID or name and turns on the output of current events associated with the task. Events are output as soon as they are generated by this task.

```
Example of starting the task with ID=1 and enabling the output of its events

kesl-control --start-task 1 -W
```

```
Display in the console information about current events that match the filter conditions

kesl-control -W --query "<filter conditions>"
```

where `<filter conditions>` is one or more logical expressions in the `<field> <comparison operation> '<value>'` format combined by the `and` logical operator.

```
Example of TaskStateChanged event output

kesl-control -W --query "EventType == 'TaskStateChanged'"
```

```
Example of TaskSettingsChanged event output initiated by the 'User' user

kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'"
```

Displaying events from the application event log

You can output information about events from the application event log to the console or a file using the command line. To output a subset of events, use filtering.

```
Output information about all events in the application event log to the console
kesl-control -E --query [--db <database file>]
```

where `<database file>` is the full path to the event log database file to output events from.

By default, the application stores information about events in the `/var/opt/kaspersky/kesl/private/storage/events.db` database. The location of the database is determined by the `EventsStoragePath` general application setting.

If the event log is in the default database, use the following command to output events to the console:

```
kesl-control -E
```

You can use `less` to navigate the list of displayed events. By default, the application stores up to 500,000 events. The maximum number of events that the application stores is determined by the `MaxEventsNumber` general application setting.

```
Display in the console information about events in the application event log that meet certain criteria
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

where:

- `<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operator> '<value>'` format combined using the logical operator `and` to restrict the results of the query.
- `<number>` is the number of the latest events in the selection (that is, the number of records counting from the end of the selection) that you want to output.
- `--json`: output events in JSON format.
- `--reverse`: display events in reverse order (from the newest event at the top to the oldest at the bottom).

```
Output information about all events in the application event log to a file
kesl-control -E --query "<>" [--db <database file>] [-n <number>] --file <path to file> [--json]
```

where `--file <path to file>` is the full path to the file to output events to.

Useful articles

What to do with false positives

Viewing reports

Viewing reports is only available in the graphical interface of the application.

Information about the operation of each Kaspersky Endpoint Security component, the performance of each scan task, the update task and integrity check task, and the overall operation of the application is recorded in *reports*.

The following event importance levels are used in reports:

- *Critical* – events with the critical importance level that need your attention as they indicate problems in the application operation or vulnerabilities in the device protection
- *High*
- *Medium*
- *Low*
- *Information*
- *Error*

The following reports are available in the application:

- **Statistics**. File Threat Protection and scan task statistics. You can update the displayed report by clicking the **Reload** button.
- **System audit**. Information about events that occur during the application operation and during the user interaction with the application.
- **Threat protection**. Information about the events that are logged while the following application components were running:
  - File Threat Protection
  - Removable Drives Scan
  - Anti-Cryptor
  - Web Threat Protection
  - Mail Threat Protection
  - Network Threat Protection
  - BadUSB Attack Prevention
  - Firewall Management
  - Application Control

- Device Control
- Behavior Detection
- Exploit Prevention
- System Integrity Monitoring
- Web Control

- **On-demand tasks**. This report contains information about events logged by scan tasks, update tasks, and system integrity check tasks.
- **Execution prevention** This report contains information about events logged during object execution prevention by the EDR Expert (on-premises) and EDR Optimum components.

How to view a report in the application interface

1. Open the main window of the application graphical interface.
2. In the lower part of the main application window, click the **Reports** button.

   The **Reports** window will open.
3. In the left part of the **Reports** window, select the required report type.

   The report is displayed in the right part of the window. Report data is presented as a table that contains a list of events. Each line in the table contains information about a separate event. Event attributes are displayed in the table columns. Events logged while various components and tasks are running have different sets of attributes.

   By default, events are sorted in ascending order by the values in the **Date and time** column. For convenient processing of reports, you can modify the presentation of data on the screen in the following ways:

   - Filter the list of events by occurrence time.
   - Use the search function to find a specific event.
4. To view detailed information about an event, select the event in the report.

   The section that contains the attributes of this event is displayed at the bottom of the window.

Obtaining system performance metrics

Kaspersky Endpoint Security affects the operating system. To help you analyze the impact, the application can obtain metrics associated with application performance.

You can analyze metrics in data visualization tools, such as Grafana. You can publish exported metrics to monitoring systems such as Prometheus and Zabbix.

```
Configure the collection of metrics for operating system resources used by the application

kesl-control [-J] --export-metrics [--period <interval in seconds between outputs>|--interactive]
```

Where:

`--period` enables periodic output of results to the command line (with the output interval specified in seconds).

`--interactive` enables interactive output (on the **Enter** key being pressed).

This command outputs the list of metrics to the console.

List of metrics

Internal name of the metric; label and type of the metric	Description and recommended threshold setting
lfs_system_descriptor_opened_count Gauge	Number of descriptors currently opened by the kesl process. If the number of descriptors grows by more than 250 per hour, we recommend contacting Technical Support.
lfs_system_uptime_milliseconds Counter	Number of milliseconds from the startup of the operating system to now.
lfs_system_memory_usage_bytes 'type=virtual' label Gauge	Amount of virtual memory currently used by the kesl process. We recommend taking steps to set a threshold based on the system information. You can get this information manually or using a script. For an example script, you can contact Technical Support.
lfs_system_memory_usage_bytes 'type=resident' label Gauge	Amount of resident memory currently used by the kesl process. We recommend taking steps to set a threshold based on the system information. You can get this information manually or using a script. For an example script, you can contact Technical Support.
lfs_system_memory_usage_bytes 'type=swap' label Gauge	The amount of swap space currently being used by the kesl process. We recommend taking steps to set a threshold based on the system information. You can get this information manually or using a script. For an example script, you can contact Technical Support.
lfs_system_memory_wd_limits_bytes 'type=virtual' label Gauge	Limit on the use of virtual memory by the kesl process.
lfs_system_memory_wd_limits_bytes 'type=resident' label Gauge	Limit on the use of resident memory by the kesl process.
lfs_system_memory_wd_limits_bytes 'type=swap' label Gauge	Limit the use of swap space by the kesl process.
lfs_system_cpu_usage_milliseconds 'type=user' label Counter	Milliseconds of CPU time used by the kesl process in user space, from the start of the kesl process to now. We recommend taking steps to set a threshold based on the system information. You can get this information manually or using a script. For an example script, you can contact Technical Support.
lfs_system_cpu_usage_milliseconds 'type=kernel' label Counter	Milliseconds of CPU time used by the kesl process in kernel space, from the start of the kesl process to now. We recommend taking steps to set a threshold based on the system information. You can get this information manually or using a script. For an example script, you can contact Technical Support.
lfs_system_cpu_usage_milliseconds 'type=total' label Counter	Milliseconds of CPU time used by the kesl process in user space and kernel space, from the start of the kesl process to now. If the CPU time used by the kesl process exceeds the rest of the workload, we recommend contacting Technical Support.
lfs_tcpSynInterceptor_connection_hanging_count Counter	Total number of network connections hanging at the handshake stage in the TCP network between the server and the client from the start of the kesl process to now (network connections are considered hanging if they have been waiting for the remote server to allow the connection for a time between 1 second to 2 minutes, depending on the system setting in /proc/sys/net/ipv4/tcp_syn_retries). An increase of this metric may be caused by the remote server being inaccessible or missing. If the number of hanging network connections grows by more than 10 per minute, we recommend contacting Technical Support.
lfs_tcpSynInterceptor_connection_count Gauge	Number of network connections currently waiting to connect to the remote server.

Internal name of the metric; label and type of the metric	Description and recommended threshold setting
lfs_tcpSynInterceptor_verdict_count "verdict=allow" label Counter	Total number of intercepted connections that have been established from the start of the kesl process to the present.
lfs_tcpSynInterceptor_verdict_count 'verdict=drop' label Counter	Total number of intercepted connections that have not been established, counting from the start of the kesl process to now.
lfs_tcpSynInterceptor_verdict_count 'verdict=unknown' label Counter	Total number of network connections from the start of the kesl process to the present moment with a solution of the remote server that cannot be processed.
lfs_tcpSynInterceptor_verdict_latency_milliseconds Histogram	Histogram of the time the remote server takes to make a solution on a connection from the time when the SYN packet is intercepted to the time when resolution is issued for it.
lfs_tproxy_connection_count 'direction=inbound' label Gauge	Current number of intercepted inbound network connections.
lfs_tproxy_connection_count 'direction=outbound' label Gauge	Current number of intercepted outbound network connections.
lfs_tproxy_connection_processed_count 'direction=inbound' label Counter	Total number of inbound network connections intercepted.
lfs_tproxy_connection_processed_count 'direction=outbound' label Counter	Total number of outbound network connections intercepted.
lfs_tproxy_connection_orphaned_count Counter	The total number of connections (from the start of Web Threat Protection, Network Threat Protection, and Web Control protection components) intercepted by Kaspersky Endpoint Security despite their interception not being intended (for example, due to an incompatible iptables configuration or the fact that the application did not have time to process a new interception configuration). Such connections are rejected. If the total number of such connections exceeds 10, which may indicate incorrect operation of the application or the system, we recommend contacting Technical Support.
lfs_tproxy_threadPool_task_count Counter	Total number of tasks (new connection, new batch of data, data sent, and so on) that have been added to the thread pool since the start of the Web Threat Protection, Network Threat Protection, and Web Control protection components. If the total number of created but uncompleted tasks keeps growing, you need to add resources, configure exclusions, or contact Technical Support.
lfs_tproxy_threadPool_thread_count Gauge	Number of threads serving the MITM mechanism of the network interceptor. Threads are created by the thread manager to handle connections. All threads execute the same code, within which they wait for network events, such as new connections and incoming packets on established connections.
lfs_tproxy_threadPool_thread_waiting Gauge	Number of free threads out of lfs_tproxy_threadPool_thread_count. Threads waiting on poll in the MITM mechanism of the network interceptor.
lfs_tproxy_threadPool_task_duration_milliseconds Histogram	Histogram of the execution time of tasks that process intercepted connections. If the execution time of 95% of tasks exceeds 1 second, you need to add resources, configure exclusions, or contact Technical Support.
lfs_tproxy_socket_count Gauge	Current number of sockets (listening sockets and connection sockets). An intercepted connection has 2 connection sockets.

Internal name of the metric; label and type of the metric	Description and recommended threshold setting
lfs_trafficScanning_object_hanging_count Gauge	Current number of hanging object scans in intercepted traffic (scans with a duration over 1 minute are considered hanging). The total number of hanging object scans exceeding 35 indicates a problem with the application databases. In such cases, we recommend contacting Technical Support.
lfs_trafficScanning_object_duration_milliseconds Histogram	Histogram of durations of intercepted traffic object scans. If the scan time for 95% of objects exceeds 1 second, you need to add resources, update application databases, or contact Technical Support. If the growth rate of packet scans in the intercepted traffic is 0 and the value of the lfs_tproxy_threadPool_task_count metric is not 0, you need to update the application databases or contact Technical Support.
lfs_fileMonitor_cache_size Gauge	Current size of the File Monitor (file revision cache), which monitors file modification. If the current File Monitor cache size is greater than 50,000, we recommend contacting Technical Support.
lfs_fileMonitor_cache_hit_count Counter	Hit count of the File Monitor cache (file revision cache), which monitors file modification.
lfs_fileMonitor_cache_miss_count Counter	Miss count of the File Monitor cache (file revision cache), which monitors file modification.
lfs_faCache_file_count Gauge	Current size of the cache of fanotify interceptor files that do not need to be scanned. If the current file cache size is greater than 100,000, we recommend contacting Technical Support.
lfs_faCache_file_hit_count Counter	Hit count of the cache of fanotify interceptor files that do not need to be scanned.
lfs_faCache_file_miss_count Counter	Miss count of the cache of fanotify interceptor files that do not need to be scanned.
lfs_faCache_volume_count Gauge	Current size of the fanotify interceptor mount point cache.
lfs_oas_cache_file_count Gauge	Current size of the cache of File Threat Protection files that do not need to be scanned. If the current file cache size is greater than 100,000, we recommend contacting Technical Support.
lfs_oas_cache_file_hit_count Counter	Hit count of the cache of File Threat Protection files that do not need to be scanned.
lfs_oas_cache_file_miss_count Counter	Miss count of the cache of File Threat Protection files that do not need to be scanned.
lfs_oas_cache_volume_count Gauge	Current size of the File Threat Protection mount point cache.
lfs_processManager_cache_size Gauge	Current number of active processes in the system that are cached.
lfs_processManager_cache_hit_count Counter	Hit count for the system process cache.
lfs_processManager_cache_miss_count Counter	Miss count for the system process cache.
lfs_blockingProcessInterceptor_cache_size Gauge	Current size of the cache of interpreters that can be used to start processes. This number depends on how intensely scripts are run on a specific device. If the current file cache size is greater than 10000, we recommend contacting Technical Support.
lfs_blockingProcessInterceptor_cache_hit_count Counter	Hit count of the interpreter cache.

Internal name of the metric; label and type of the metric	Description and recommended threshold setting
lfs_blockingProcessInterceptor_cache_miss_count Counter	Miss count of the interpreter cache.
lfs_doc_prevention_cache_file_count Gauge	Current size of the *Execution Prevention for objects* task file cache for objects that do not need scanning (when opening documents).
lfs_script_prevention_cache_file_count Gauge	Current size of the *Execution Prevention for objects* task file cache for objects that do not need scanning (when running scripts).
lfs_doc_prevention_cache_file_hit_count Counter	Number of hits in the *Execution Prevention for objects* task file cache for objects that do not need scanning (when opening documents).
lfs_script_prevention_cache_file_hit_count Counter	Number of hits in the *Execution Prevention for objects* task file cache for objects that do not need scanning (when running scripts).
lfs_doc_prevention_cache_file_miss_count Counter	Number of misses in the *Execution Prevention for objects* task file cache for objects that do not need scanning (when opening documents).
lfs_script_prevention_cache_file_miss_count Counter	Number of misses in the *Execution Prevention for objects* task file cache for objects that do not need scanning (when running scripts).
lfs_doc_prevention_cache_volume_count Gauge	The current size of the mount point cache for the "Execution prevention for objects" task for documents.
lfs_script_prevention_cache_volume_count Gauge	The current size of the mount point cache for the "Execution prevention for objects" task for scripts.
eka_telemetry_metrics_registry_callbacks_exec_duration_milliseconds Gauge	How long the current metrics update took for all clients registered in the registry (in milliseconds).
eka_telemetry_metrics_registry_registered_callbacks Gauge	Current number of metric update callbacks that the MetricsRegistry has performed for all registered clients.
eka_telemetry_metrics_registry_scrape_duration_milliseconds Gauge	How long it took to get all registry metrics (in milliseconds). If 99% of the values of this metric exceed 1 second for a 10-minute period, we recommend contacting Technical Support.

Application stability monitoring

Kaspersky Endpoint Security application stability monitoring tracks the number of abnormal application halts and notifies the administrator of unstable application performance.

How to configure Application stability monitoring in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security for Linux policy.

   The policy properties window opens.
3. Go to the **Application settings** tab.
4. Select **General Settings** → **Performance**.
5. Select or clear the **Enable monitoring of application stability** check box. This check box is cleared by default.

How to configure Application stability monitoring in the Administration Console

1. In the tree of the Kaspersky Security Center Administration Console, in the **Managed devices** folder, open the folder with the name of the administration group that includes the required devices.

2. In the workspace, select the **Policies** tab.

3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.

4. Go to the **General settings** → **Application settings** section.

5. Select or clear the **Enable monitoring of application stability** check box. This check box is cleared by default.

> To apply this setting, the application and the Network Agent must be restarted.

If the application is unstable, the following message is displayed in the properties of the device with the installed application: *<Number> abnormal halts of the application since <date and time>*.

How to configure Application stability monitoring on the command line

On the command line, you can configure Kaspersky Endpoint Security stability monitoring using the `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash`, and `WarnRemovingThreshold` settings in the kesl.ini configuration file.

The `TrackProductCrashes` allows enabling the sending of device status information from Kaspersky Endpoint Security to Kaspersky Security Center when the application is unstable. This setting can take the following values:

- `Yes/true` enables the sending of device status information from Kaspersky Endpoint Security to Kaspersky Security Center.

- `No/false` disables the sending of device status information from Kaspersky Endpoint Security to Kaspersky Security Center.

The `ProductHealthLogFile` setting lets you specify the path to a file used for application stability monitoring. Default value: /var/opt/kaspersky/kesl/private/kesl_health.log.

The `WarnThreshold` setting lets you set the time interval (in seconds) in which the application must experience the specified number of abnormal halts before displaying a notification about unstable operation. Default value: 3600 seconds.

The `WarnRemovingThreshold` setting lets you set the time interval (in seconds) after which the application's unstable status will be cleared. Default value: 86400 seconds.

The `WarnAfter_#_crash` setting lets you set the number of abnormal halts of the application after which a notification is displayed about application instability. The setting can take values from 0 to 10. Default value: 10. If the value is 0, an unstable application notification is not displayed.

> After making changes to this file, restart Kaspersky Endpoint Security.

Application components integrity check

Kaspersky Endpoint Security contains many various binary modules in the form of dynamic linked libraries, executable files, configuration files, and interface files. A hacker can replace one or more executable modules or files of the application with other files containing malicious code. To prevent such replacement of modules and files, Kaspersky Endpoint Security can check the integrity of application components. The application checks modules and files for unauthorized changes or corruption. If an application module or file has an incorrect checksum, it is considered to be corrupted.

An integrity check is run for the following application components if installed on the device:

- application package
- Graphical user interface package
- Kaspersky Security Center Network Agent package
- Kaspersky Endpoint Security management web plug-in
- Kaspersky Endpoint Security MMC management plug-in

The integrity of the application components is checked using an integrity check utility. The utility checks integrity of the files in the special lists called *manifest files*. Each application component has its own manifest file that contains a list of application files whose integrity is important for correct operation of this application component. The manifest files are digitally signed and their integrity is checked as well.

To run the integrity check utility on Linux devices, an account with root privileges is required.

The integrity check utility is installed with the application and located at the following paths:

- As part of the application package (integrity_checker): /opt/kaspersky/kesl/bin/integrity_checker.
- As part of the MMC management plug-in for Kaspersky Endpoint Security (integrity_checker.exe):
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version number>.plg\integrity_checker.exe – for 32-bit operating systems
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<version number>.plg\integrity_checker.exe – for 64-bit operating systems

The manifest files are located at the following paths:

- To check the integrity of the application package: /opt/kaspersky/kesl/bin/integrity_check.xml.
- To check the integrity of the graphical user interface package: /opt/kaspersky/kesl/bin/gui_integrity_check.xml.

- To check Network Agent:
  - /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – for 32-bit operating systems
  - /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – for 64-bit operating systems
- To check the Kaspersky Endpoint Security MMC management plug-in
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plugin version>.plg\integrity_check.xml – for 32-bit operating systems
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plugin version>.plg\integrity_check.xml – for 64-bit operating systems

To check the integrity of a solution component, you need to run the tool from the folder of that component's tool.

```
Check the integrity of the application package

integrity_checker [<path to manifest file>] --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type
kds-with-filename
```

```
Check the integrity of the graphical interface package

integrity_checker <path to manifest file> --crl /var/opt/kaspersky/kesl/private/data/KDSCRL/ --signature-type kds-
with-filename
```

```
Check the integrity of the Kaspersky Endpoint Security MMC management plug-in

integrity_checker.exe [<path to manifest file>]
```

```
Check the integrity of Network Agent

integrity_checker <path to manifest file>
```

The default path is for a manifest file located in the same directory as the integrity checker utility.

You can run the utility with the following optional settings:

- `--crl <directory>` is the path to the directory containing the Certificate Revocation List.
- `--verbose` – display detailed information about performed actions and their results. If you do not specify this setting, only errors, objects that did not pass the check, and scan statistics summary will be displayed.
- `--trace <file name>` writes the events that occurred during the scan to the specified file with the DEBUG logging level.
- `--signature-type kds` is the type of signature to be verified (this option is required for checking the Kaspersky Endpoint Security management web plug-in).
- `--signature-type kds-with-filename` is the type of the signature to be verified (this setting is required for checking the application package and the graphical interface package).

- `--single_file <file name>` checks only the specified file in the manifest and ignore all the other objects of the manifest.

- `--version` – display the version of the utility and do not perform an integrity check.

```
View all available options of the integrity checker tool

integrity_checker --help
```

The result of checking the manifest files is displayed as follows:

- `SUCCEEDED` — integrity of the files has been confirmed (return code 0).

- `FAILED` – integrity of the files has not been confirmed (return code is not 0).

If a violation of the integrity of the application or Network Agent is detected when the application starts, Kaspersky Endpoint Security generates the corresponding event in the event log and in Kaspersky Security Center.

Application access control

Access control in Kaspersky Endpoint Security is based on a Role Based Access Control (RBAC) policy. To grant a user certain rights or access to a resource, you need to assign corresponding roles. A *role* is a set of rights and privileges for managing the application.

User roles makes routine management of access rights easier and quicker. Access rights for a role are configured in accordance with typical tasks and job descriptions of users.

The application needs elevated privileges in the operating system to protect devices. The application requires root privileges to perform some of its basic security functions.

The role-based access model of the application includes the Administrator (admin) role. In certain cases, the actions of users with the Administrator role may lead to operations being performed with privileges of the operating system superuser (root).

The Administrator role should only be granted to trusted users. Compromise or abuse of this Administrator role leads to the compromise of the entire device and can impact the security, integrity, or performance of your organization's infrastructure, as well as user data.

Granting the Administrator role is the responsibility of the owner of the system and should be carried out in accordance with the access control policy of your organization and the level of trust towards the relevant users.

Predefined roles

Access to Kaspersky Endpoint Security functions via the command line is provided to users in accordance with their roles. A *role* is a set of rights and privileges for managing the application.

Four groups of system users are created in the operating system:

- kesladmin
- kesluser
- keslaudit
- nokesl

When you assign an application role to a system user, the user is added to the corresponding group (see the table below). When you revoke a role from a user, this user is removed from the corresponding group.

After assigning or revoking a role, you must restart the application (the kesl process) and its graphical interface (the kesl-gui process).

Roles and user groups

Role name	Role in application	OS user group	Permissions
Administrator	admin	kesladmin	Managing application settings and task settings in the graphical interface of the application and on the command line without using the `sudo` command. Manage application licensing. Assigning roles to users. Revoking roles from users (an administrator cannot revoke the admin role from themselves). View and manage users' Storages.
User	user	kesluser	Manage only user file scan tasks. Start and stop Update tasks. Sending files to Sandbox for scanning View reports for the tasks created by this user. View specific events that are common for all application users.
Auditor	audit	keslaudit	Viewing application settings View application status. View all tasks, their settings, and start schedules. View all events. View all objects in Backup.
–	–	nokesl	No role is assigned in the application, no permissions.

How to assign or revoke a user role

Roles define a user's rights and actions that the user can perform in the system. Only users with the Administrator (kesladmin) role can manage roles. We recommend creating at least one user with the Administrator role on the protected device to avoid having the application managed by users with root privileges.

Viewing a list of users and roles

```
kesl-control --get-user-list
```

Assign a role to a user

```
kesl-control --grant-role <admin|user|audit> <user name>
```

Example of assigning the audit role to user test15

```
kesl-control --grant-role audit test15
```

Revoke a role from a user

```
kesl-control --revoke-role <role> <user name>
```

Example of revoking the audit role from user test15

```
kesl-control --revoke-role audit test15
```

RBAC functional areas in Kaspersky Security Center

By default, users with the "Kaspersky Endpoint Security Administrator" role in the Kaspersky Security Center administration system have access to all functionality of Kaspersky Endpoint Security.

You can select one of the following predefined levels of access to Kaspersky Endpoint Security functionality for a Kaspersky Endpoint Security user or group:

- **Read** grants the ability to view the general settings of Kaspersky Endpoint Security and the settings of Kaspersky Endpoint Security components.
- **Edit** grants the ability to view and edit the general settings of Kaspersky Endpoint Security and the settings of Kaspersky Endpoint Security components.
- **Execute** grants the ability to start and stop Kaspersky Endpoint Security tasks.
- **Perform operations on device selections** grants the ability to start and stop Kaspersky Endpoint Security tasks for a selection of devices.

You can also configure advanced access permissions: allow or deny access to Kaspersky Endpoint Security functions.

How to configure access permissions for application functions in the Web Console

1. In the main window of the Web Console, select **Users & roles** → **Role**.
2. Select the role for which you want to configure functional areas.
   If necessary, you can add a new role. See Kaspersky Security Center Help for more details.
3. Configure access rights to the Kaspersky Endpoint Security application.
4. Click the **Save** button.

Access permissions for Kaspersky Endpoint Security functions

Functional area	Kaspersky Endpoint Security functionalities
Basic functionality	Updating application databases and modules Rollback Inventory BadUSB Attack Prevention System Integrity Monitoring System Integrity Check Detection settings Kaspersky Security Network User interaction Performance Network settings Container Scan Technical Support Reports and Storage Integration with KSC Telemetry source and auditd mode (OS interaction settings) Event settings Light Agent mode Add a key
Application Control	Application Control
Device Control	Device Control
Data Encryption	Grant temporary access to a device (Device Control)
Trusted zone	Trusted zone: • Specifies trusted web addresses • Trusted IP addresses • Monitored ports • Trusted root certificates • Trusted domains • Trusted mount points • Traffic interception exclusions • Trusted applications • Malware Scan exclusions • Trusted devices

Functional area	Kaspersky Endpoint Security functionalities
Detection and Response	Built-in agents: • Managed Detection and Response • Endpoint Detection and Response • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Integration with KUMA. Response actions: • Terminate process • Start process • IOC Scan • Receive file from device • Move file to Quarantine • Delete file from device • Network isolation • Execution prevention for objects • Telemetry settings
Host Intrusion Prevention	Behavior Detection Exploit Prevention Anti-Cryptor Network Threat Protection Firewall Management
Protection components	Malware Scan Critical Areas Scan File Threat Protection Mail Threat Protection Removable drives scan Web Threat Protection
Web Control	Web Control

Recommendations for typical roles of protected devices

Workstation

If you are installing the application on a workstation, we recommend also installing the graphical interface of the application.

After installing the application:

- Enable Web Threat Protection.
- If the device does not have a direct connection to the internet, select local certificate validation in the network traffic scan settings using one of the following options:
  - In the Web Console, under **Encrypted Connections Scan**, click the **Settings** button and then set **Certificate verification policy** to **Local check**.
  - In the Administration Console, under **Settings for encrypted connections**, set **Certificate verification policy** to **Local check**.
  - Locally on the device using the command line:

```
kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
```

The application will not use the internet to verify certificates.

- Configure an exclusion from file operation interception (global exclusion) for all remote directories mounted on the device using the Samba and NFS protocols.

File server

After installing the application:

1. Make sure that the scanning of archives is disabled in the File Threat Protection settings. This option is selected by default.
2. Create a *Malware Scan* task with the following settings:
   - scanning archives: enabled
   - task schedule: during minimum load hours

Web server

Kaspersky Endpoint Security is not intended for web server protection. To protect web servers, we recommend using Kaspersky NGFW and Kaspersky Web Traffic Security.

If you are using Kaspersky Endpoint Security on a web server, if the server uses the HTTPS protocol and has a high client load, Web Threat Protection may significantly increase the utilization of system resources. This is caused by the application decrypting and scanning HTTPS traffic.

Analyze how the load on the web server changes while Web Threat Protection is working. You can configure exclusions to optimize settings and eliminate compatibility issues.

Proxy server

After installing the application, disable the Web Threat Protection and Network Threat Protection components on the device that acts as a proxy server or load balancer.

Server with containerization

After installing the application, disable the Web Threat Protection, Network Threat Protection, and Firewall Management components on servers that are used for containerization services. To protect container environments, you can use the Kaspersky Container Security application.

Database server

Configure global exclusions for the working directories of the database management system.

> Check with your DBMS administrator for the list of working directories in your infrastructure.

> The following example paths are intended for the Ubuntu operating system. In other operating systems, the directories may differ.

Recommendations for popular DBMS

PostgreSQL. It is critically important to completely eliminate any latency for file operations with data files and write-ahead logs (WAL files). We recommend also excluding file operations of PostgreSQL processes and tablespaces (see the example below). In a typical PostgreSQL installation, these files are located in the following directories:

- Statistics and parallel queries: `/dev/shm`
- Data: `/var/lib/postgresql/<PostgreSQL version>/main`
- WAL files: `/var/lib/postgresql/<PostgreSQL version>/main/pg_wal`
- Executable files: `/usr/lib/postgresql/<PostgreSQL version>/bin/`.

Postgres Pro. Follow the guidelines for PostgreSQL. Additionally, add the `/var/lib/pgpro/<Postgres Pro version>/data` directory to the exclusions.

Oracle Database. You can get a list of working directories for all databases from the `/etc/oratab` configuration file.

ScyllaDB. When using the Web Threat Protection and Network Threat Protection components, use the eBPF mode of traffic interception. To manage the caching mode of Detection and Response solutions, use the default value of the `UseIncreasedXdrEventsCache=yes` setting in the kesl.ini configuration file.

Example for configuring global exclusions for PostgreSQL working directories

If you are using a mechanism based on *fanotify technology* to intercept system events, the DBMS file directories must be mount points. If you use the *updatable kernel module* to intercept system events, you do not need to create mount points.

To create mount points:

1. Check if the directories with database file are mount points:

   ```
   mount
   ```

   If the directories are absent from the output of the mount command:

   a. Create a mount point:

   ```
   mount --bind /var/lib/postgresql/<PostgreSQL version>/main/ /var/lib/postgresql/<PostgreSQL version>/main
   ```

   You do not need to create a separate mount point for the directory with WAL files because it is nested inside the data directory.

   b. Add the following line to the /etc/fstab file to make the newly created mount point persist in the system after restart:

   ```
   /var/lib/postgresql/<PostgreSQL version>/main /var/lib/postgresql/<PostgreSQL version>/main none
   defaults,bind 0 0
   ```

2. Restart the PostgreSQL service:

   ```
   systemctl restart postgresql
   ```

To configure global exclusions for working directories:

1. Add the directories to global exclusions:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/var/lib/postgresql/<PostgreSQL version>/main
kesl-control --set-app-settings ExcludedMountPoint.item_0001=/var/lib/postgresql/<PostgreSQL
version>/main/pg_wal
kesl-control --set-app-settings ExcludedMountPoint.item_0002=/usr/lib/postgresql/<PostgreSQL version>/bin/
kesl-control --set-app-settings ExcludedMountPoint.item_0003=/usr/lib/postgresql/<PostgreSQL version>
```

2. If you use tablespaces, add them to exclusions as well:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=<tablespace directory>
```

3. Restart the application to apply global exclusions:

```
systemctl restart kesl
```

Updating application databases and modules

Updating the databases and application modules of Kaspersky Endpoint Security ensures up-to-date protection on your device. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Endpoint Security databases contain information about threats and ways of neutralizing them. To detect threats quickly, you are urged to regularly update the application databases and modules.

> Current application license is required for regular database updates. If there is no current license, you will only be able to perform one update.

If application deployment was successful and you chose to update the databases at the initial configuration stage, then after installing the application, the databases are up to date. You can get information about the status of databases when viewing the protection status of the device in Kaspersky Security Center by looking at the statuses of client devices and on the command line using the `kesl-control --app-info` command. If the databases are not up to date, you need to configure and initiate a database update.

Configuring database and module updates

1. **Selecting an update distribution scheme and update source**

   An *update source* is a resource that contains updates for Kaspersky Endpoint Security databases and application modules. The update source can be one of the following: Kaspersky update servers; Kaspersky Security Center Administration Server storage; an FTP, HTTP, or HTTPS server; a local or network directory mounted by the user using the Samba or NFS protocols.

   > If Kaspersky Endpoint Security is used in Light Agent mode, the databases on the protected virtual machines are updated from the directory on the SVM.

2. Configuring the database update task

   The *Update* task downloads the update package and installs database and application module updates on the device.

The update functionality (including anti-virus signature updates and code base updates) may not be available in the application in the territory of the USA.

During an update, the following objects are downloaded and installed on your device:

- Kaspersky Endpoint Security databases. Application databases include malware detection rules, a description of network attacks, databases of malicious and phishing web addresses, databases of banners, spam databases, and other data.
- Application modules. Module updates are intended to eliminate vulnerabilities in the application and to improve methods of protecting devices. Module updates may change the behavior of application components and add new capabilities.

You can also receive automatically installed application updates (autopatches). Autopatches contain fixes and improvements for the application.

While updating, the application modules and databases on your computer are compared against their up-to-date versions at the update source. If your current databases and application modules differ from their respective up-to-date versions, the missing portions of the updates will be installed on your device.

If the databases are obsolete, the update package may be large, which may cause additional Internet traffic (up to several dozen MB). The amount of the disk space can be up to 3 GB.

Useful articles

Troubleshooting application database and module updates

What to do if you get the status: "An application update or cryptossl module update was installed. Restart the application."

How to select the update source and distribution scheme

Selecting a Kaspersky Endpoint Security update source

An *update source* is a resource that contains updates for Kaspersky Endpoint Security databases and application modules.

The update source can be one of the following: Kaspersky update servers, the storage of the Kaspersky Security Center Administration Server, a local or network (SMB/NFS) directory mounted by the user, FTP, HTTP, or HTTPS servers. When choosing your own HTTPS server as the update source, you need to make sure that it has the correct certificate chain. A self-signed certificate can only be used as the root certificate in a certificate chain. In this case, you need to add it to the list of trusted certificates on the device.

> If Kaspersky Endpoint Security is used in Light Agent mode, the databases on the protected virtual machines are updated from the directory on the SVM.

If several resources are selected as update sources, Kaspersky Endpoint Security tries to connect to them one after another, starting from the top of the list, and performs the update task by retrieving the update package from the first available source. You can configure the response timeout of a selected update source when attempting to connect to it. If an update source does not respond within the specified time, the application contacts the next update source in the list.

Selecting an update distribution scheme

Kaspersky Endpoint Security supports the following distribution schemes for updates of databases and application modules:

Centralized update

If you use Kaspersky Security Center to centrally manage device protection in your organization, we recommend setting up centralized database updates. Centralized update reduces external Internet traffic, and provides for convenient monitoring of the update.

Centralized update consists of the following steps:

1. Download the update package to a repository within the organization's network.

   You can use the repository of the Kaspersky Security Center Administration Server as the repository. The update package is downloaded to the Administration Server repository via the *Download updates to Administration Server repository* task of the Administration Server.

2. Distribute the update package to client devices

   The update package is distributed to the client devices by the *Update* task of Kaspersky Endpoint Security. In the task settings, select Kaspersky Security Center as the update source.

Update from Kaspersky update servers

Kaspersky update servers are located in different countries around the world, which ensures a high reliability of updates. If an update cannot be performed from one server, the application switches over to the next server. Updates are downloaded via HTTPS protocol. For more information about Kaspersky update servers, refer to the Technical Support Knowledge Base.

Updating from a local or network directory (SMB/NFS) mounted by a user, or from an FTP, HTTP, or HTTPS server

The custom update source must contain pre-downloaded update packages (which you can do, for example, using the Kaspersky Update Utility). When choosing your own HTTPS server as the update source, you need to make sure that it has the correct certificate chain. A self-signed certificate can only be used as the root certificate in a certificate chain. In this case, you need to add it to the list of trusted certificates on the device. You can specify a custom update source in *Update* task settings. For more details about creating custom update sources, refer to the Kaspersky Security Center Help.

Updates are downloaded from Kaspersky update servers or from other FTP, HTTP, or HTTPS servers over standard network protocols. By default, Internet connection settings are determined automatically. If you are using a proxy server, specify the proxy server settings.

How to configure the database update task

The *Update* task downloads the update package and installs database and application module updates on the device.

Updating databases in Kaspersky Security Center

In Kaspersky Security Center, the *Update* task is created automatically by the Administration Server Quick Start Wizard. To create the *Update* task while running the Wizard, you need to install the Kaspersky Endpoint Security management plug-in.

You can use an automatically created *Update* group task or create and run custom group and local update tasks using the Web Console or Administration Console.

If Kaspersky Endpoint Security is used in Light Agent mode, databases on protected virtual machines are updated using a special *Update* local task, where the directory on the SVM is specified as the update source. The update task starts automatically. You cannot delete this task or change its settings. Updating databases and application modules using tasks created in Kaspersky Security Center is not supported.

How to configure and run an update task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. In the list of tasks, select the Kaspersky Endpoint Security update task and click the name of the task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. In the **Update sources** section, select the source from which the application will receive updates for databases and modules, depending on the update scenario used.

   The list of update sources contains two sources: Kaspersky update servers and Kaspersky Security Center. The **Status** column indicates whether the application is using this update source when running the task. You can add other update sources to the list by clicking the **Add** button. As update sources, you can specify directories on FTP, HTTP, and HTTPS servers or directories on any device mounted on the protected client device, including directories on remote devices mounted via the Samba or NFS protocols. If an update cannot be performed from an update source, Kaspersky Endpoint Security switches to the next update source. The application accesses update sources in the order in which they appear in the table.

5. In the task properties window, select the **Schedule** tab and configure the schedule for running the update task. By default, start in manual mode is selected for the task.

   If you have selected **Kaspersky Security Center** as the update source, select **When downloading updates to the repository** from the **Start task** drop-down list. For more details about scheduling tasks, refer to the Kaspersky Security Center Help.

6. Save your changes.

The task will start according to the configured schedule. You can also run the task manually.

How to configure and run an update task in the Administration Console

1. In the Administration Console, perform one of the following actions:

   - To edit the settings of a task that is run on devices included in the specified administration group, select this administration group in the console tree, then select the **Tasks** tab in the workspace.

   - To edit the settings of a task that is run on one or multiple devices (a task for a set of devices), select the **Tasks** folder in the console tree.

2. In the list of tasks, select an update task and double-click it to open the task properties window.

3. In the task properties window, select the **Update sources** section in the list on the left.

4. In the table, select the update source from which the application will receive updates for databases and modules, depending on the update scenario used.

   The list of update sources contains two sources: Kaspersky update servers and Kaspersky Security Center. The **Status** column indicates whether the application is using this update source when running the task. You can add other update sources to the list by clicking the **Add** button. You can specify FTP-, HTTP-, or HTTPS servers as update sources. If an update cannot be performed from an update source, Kaspersky Endpoint Security switches to the next update source. The application accesses update sources in the order in which they appear in the table.

5. Select the **Settings** section and configure other update settings.

6. Select the **Schedule** tab and configure the schedule for running the update task. By default, start in manual mode is selected for the task.

   If you have selected **Kaspersky Security Center** as the update source, select **When downloading updates to the repository** from the **Scheduled start** drop-down list. For more details about scheduling tasks, refer to the Kaspersky Security Center Help.

7. Click **Apply** or **OK** in the **Properties: <Task name>** window to save the changes made.

The task will start according to the configured schedule. You can also run the task manually.

Updating databases on the command line

On the command line, you can update databases and application modules using the *`Update`* predefined task or create user tasks of the `Update` type.

You can to manage manual update tasks (start, stop, suspend, and resume), configure the task schedule, and manage update settings by changing the settings of tasks.

How to create and configure an update task on the command line

On the command line, you can create and configure a custom update task in two ways:

- Create a task by specifying all its settings for it in a configuration file.
- Create a task with default settings and then configure its settings.

Create an update task with settings taken from a configuration file

```
kesl-control --create-task <task name> --type <task type> --file <path to file> [--json]
```

Where:

- `<path to file>` is the full path to the configuration file with the settings that you want to use for the task.
- `--json` is specified to import the settings from the configuration file in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

Example of a configuration file

```
ConnectionTimeout=10
ApplicationUpdateMode=DownloadOnly
[Sources.item_0000]
Enabled=Yes
SourceType=Custom
URL=https://s00.upd.kaspersky.com
```

To create and configure an update task with default settings:

1. Create a task by running the following command:

   ```
   kesl-control --create-task <update task name> --type Update
   ```

   Where `<update task name>` is the name that you want to set for the new update task.

   This command creates an update task with default settings.

2. If necessary, manage update task settings by running the following command:

   ```
   kesl-control --set-settings <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

3. If necessary, manage update task schedule settings by running the following command:

   ```
   kesl-control --set-schedule <update task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

4. Check the current values of task settings by running the following command:

   ```
   kesl-control --get-settings <update task ID|name>
   ```

Updating databases in the graphical interface of the application

How to start or stop an update task in the graphical interface

1. Open the main window of the application graphical interface.
2. In the main application window, click **Update**.

   The **Update** window opens.
3. Do one of the following:
   - To start a task, click the **Start** button under the task that you want to start.

     The progress of the running update task is displayed.
   - To stop a task, click the **Stop** button under the scan task that you want to stop.

     The Update task stops.
4. To view the report on the task, click the **Show report** button.

How to update using the Kaspersky Update Utility

To reduce Internet traffic, you can configure updates of application databases and modules on devices of the organization's LAN from a shared directory by using the Kaspersky Update Utility. For this purpose, one of the devices in the organization's LAN must receive update packages from the Kaspersky Security Center Administration Server or from Kaspersky update servers and use the utility to copy the received update packages to the shared directory. Other devices on the organization's LAN will be able to receive the update package from this shared directory.

To configure Kaspersky Security Center to update databases from a shared directory using the Kaspersky Update Utility:

1. Install Kaspersky Update Utility on one of the devices of the organization's LAN.

   You can download the Kaspersky Update Utility distribution kit from the Kaspersky Technical Support website.
2. Configure copying of the update package to the shared directory in the Kaspersky Update Utility settings.

   Select the update source (for example, the Administration Server repository) and the shared directory to which the Kaspersky Update Utility will copy update packages. For detailed information about using Kaspersky Update Utility, refer to Kaspersky Knowledge Base.
3. Configure updates of application databases and modules from the specified shared directory on other devices in the organization's local network:

   a. Open the properties of the **Update** task that will be performed on the required device using the Web Console or using the Administration Console.

   b. In the task properties, go to the **Update sources** section.

   c. In the **Update sources** section, select the **Other sources on the local or global network** option.

d. In the table of update sources, click the **Add** button and specify the path to the shared directory.

> The address of the update source must match the address specified in the Kaspersky Update Utility settings.

e. Select the **Use this source** check box and click **OK**.

f. In the table, set the order of the update sources using the **Up** and **Down** buttons.

g. Save the changes to the task settings.

To configure Kaspersky Security Center to update databases from a shared directory using the command line:

1. Install Kaspersky Update Utility on one of the devices of the organization's LAN.

   You can download the Kaspersky Update Utility distribution kit from the Kaspersky Technical Support website.

2. Configure copying of the update package to the shared directory in the Kaspersky Update Utility settings.

   Select the update source (for example, the Administration Server repository) and the shared directory to which the Kaspersky Update Utility will copy update packages. For detailed information about using Kaspersky Update Utility, refer to Kaspersky Knowledge Base.

3. Configure updates of application databases and modules from the specified shared directory on other devices in the organization's local network: in the `Update` task settings, set `SourceType=Custom` and specify the path to the shared directory in the `[Sources.item_#]` section.

   > The address of the update source must match the address specified in the Kaspersky Update Utility settings.

How to roll back updates of application databases and modules

After the databases and application modules are updated for the second time, the function of rolling back the databases and application modules to their previous versions becomes available.

Each time that a user starts the update process, Kaspersky Endpoint Security creates a backup copy of the current databases and application modules. This lets you roll back the databases and application modules to their previous versions when necessary. Rolling back the last update is useful, for example, if a new database version causes a false positive that results in Kaspersky Endpoint Security blocking a safe application.

> If Kaspersky Endpoint Security is used in Light Agent mode, the task cannot be used to rollback database updates.

In Kaspersky Security Center, you can create rollback tasks for administration groups or for individual devices using the Web Console or the Administration Console.

On the command line, you can roll back a database update in the following ways:

- Run the *Rollback* predefined task.
- Create and run a *Rollback* custom task.

The *rollback* task does not have any settings.

How to roll back an update of application databases and modules in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select the name of the application.

   b. In the **Task type** drop-down list, select **Rollback**.

   c. In the **Task name** field, enter a name for the new task.

   d. Under **Devices to which the task will be assigned**, select how you want to define a scope for the task.

4. Select devices according to your preferred task scope definition method.

5. Finish the wizard.

   A new task will be displayed in the list of tasks.

6. Select the check box next to the task and click the **Start** button.

How to roll back an update of application databases and modules in the Administration Console

1. In the Administration Console, perform one of the following actions:

   - To create a task that will be run on devices included in the selected administration group, select this administration group in the console tree in the **Managed devices** folder, then select the **Tasks** tab in the workspace and click the **New task** button.

     The New task wizard starts for devices of the selected administration group.

   - To create a task that will be performed on one or multiple devices (a task for a set of devices), select the **Tasks** folder in the console tree and click the **New task** button in the workspace.

     The New task wizard starts for the set of devices.

2. At the first step of the wizard, select Kaspersky Endpoint Security in the list and the **Rollback** task type.

3. If you are creating a task for a set of devices, the wizard prompts you to select the devices to which you want to assign the task. Select how you want to define the scope for the task.

4. Select devices according to your preferred task scope definition method.

5. Configure a schedule for the task.

6. Enter a name for the new task.

7. Finish the wizard.

   A new task will be displayed in the list of tasks.

8. In the list of tasks, select the task, open the context menu of the task, and select **Start**.

How to roll back an update of application databases and modules on the command line

Execute the command:

```
Roll back database and module updates
```

```
kesl-control --start-task 7
```

How to roll back an update of application databases and modules in the graphical interface

1. Open the main window of the application graphical interface.
2. In the main application window, click **Update**.

   The **Update** window opens.

3. Click the **Roll back update** link to roll back the database update.

Host Threat Protection

File Threat Protection

File Threat Protection provides a minimum level of security to the computer. The component is started together with Kaspersky Endpoint Security and scans files in real time.

How File Threat Protection works

1. **The application intercepts file operation events and blocks actions until the scan finishes.**

   The application uses a file operation interception mechanism and blocks all access to the file until the scan finishes.

2. **The application scans the file**

   File Threat Protection scans a file using the following technologies:

   - Anti-virus databases.
   - Cloud services of Kaspersky Security Network.
   - The Heuristic analysis technology allows detecting threats that are not yet covered by Kaspersky databases.

3. **Completion of the scan**

   After the scan, the application either allows the operation or blocks it and performs the action specified on threat detection.

Initial configuration of File Threat Protection

Initial configuration includes the necessary steps for basic endpoint protection.

1. **Select a system event interception mechanism**

   File Threat Protection intercepts file operation events and blocks actions until the scan finishes.

   When installing the application, you selected a system event interception mechanism:

   - Interception mechanism based on an updatable kernel module
   - System interception mechanism based on fanotify
   - Kernel module for File Threat Protection on an operating system without fanotify

   The choice of the system event interception mechanism depends on the configuration of the computer. The interception technology that offers the greatest performance is the updatable kernel module. You can enable this mechanism in the application settings.

2. **Configure File Threat Protection**

   By default, File Threat Protection is enabled and runs with settings recommended by Kaspersky experts. Default settings provide recommended protection level and optimal resource use. If you have special requirements for infrastructure security, you can change these settings.

3. **Configure the protection scope**

   By default, the application scans all files on a protected device. If you only need to scan an individual directory (for example, the directory into which files are automatically downloaded from an external source), you can specify only that directory as the protection scope. In other cases, we recommend keeping the default protection scope and using exclusions to fine-tune the scope.

4. **Exclude mount points from scanning**

   Excluding mount points from scanning allows you to refrain from intercepting file operations in a certain directory. For example, you can exclude shared network resources from the scan and use Kaspersky Endpoint Security to protect them on the device where those resources are physically stored. You can also refer to the Recommendations for File Threat Protection and scan tasks.

5. **Add exclusions**

   Exclusions help balance system security with performance. For stable operation of third-party software, add to exclusions files and directories which are listed in the documentation for the respective software.

   We recommend excluding the following objects:

   - Databases. Large databases require a lot of resources to scan. Frequent access to database files triggers frequent scans.
   - Files that resource-intensive processes work with. Scanning such files slows down the computer.
   - Directories with log files. The operating system writes to the log file all the time. As a result, File Threat Protection wastes computer resources on scanning logs.

If an object is excluded from scanning by the File Threat Protection component, we recommend scanning such objects using the *Malware Scan* task.

Additional configuration for high-load servers

Additional configuration includes steps for fine-tuning File Threat Protection. After the initial configuration, if you encounter any lag or if you are configuring high-load servers, follow these steps:

1. **Disable file access blocking during scans**

   By default, File Threat Protection blocks all access to the file being scanned until the scan finishes. If you disable blocking mode, File Threat Protection works in inform mode. This mode of file operation interception has less impact on system performance while scanning, but there is a risk that the threat in the file might not get disinfected or deleted.

   If blocking mode is disabled, Device Control, the Execution prevention for objects action, and the Removable Drives Scan task also work in inform mode.

2. **Collect file scan statistics**

   Monitor the main performance metrics of the computer: the CPU load, the performance of third-party software, or other indicators. This will help you determine how to reduce the load on the system.

   You can get file scan statistics using application performance analysis tools. You can also use your own monitoring tools.

3. **Optimize application performance**

   After analyzing the gathered information, optimize application performance:

   - Add global exclusions
   - Add exclusions
   - Optimize application settings

4. **Enable file access blocking during scans**

   Enable file access blocking during scans. When an infected object is detected, the application will perform the selected action.

Special considerations and limitations

- If the root user does not have access to a file in a remote directory mounted on the device over the NFS4 protocol, the application blocks access to such a file for all users.
- If File Threat Protection and Container monitoring are enabled, the application also scans all namespaces and containers.

How to create a protection scope

A *protection scope* is a list of paths to objects that Kaspersky Endpoint Security scans for threats. By default, the application scans all files on a protected device. If you only need to scan an individual directory (for example, the directory into which files are automatically downloaded from an external source), you can specify this directory as the protection scope. In other cases, we recommend keeping the default protection scope and using exclusions to fine-tune the scope.

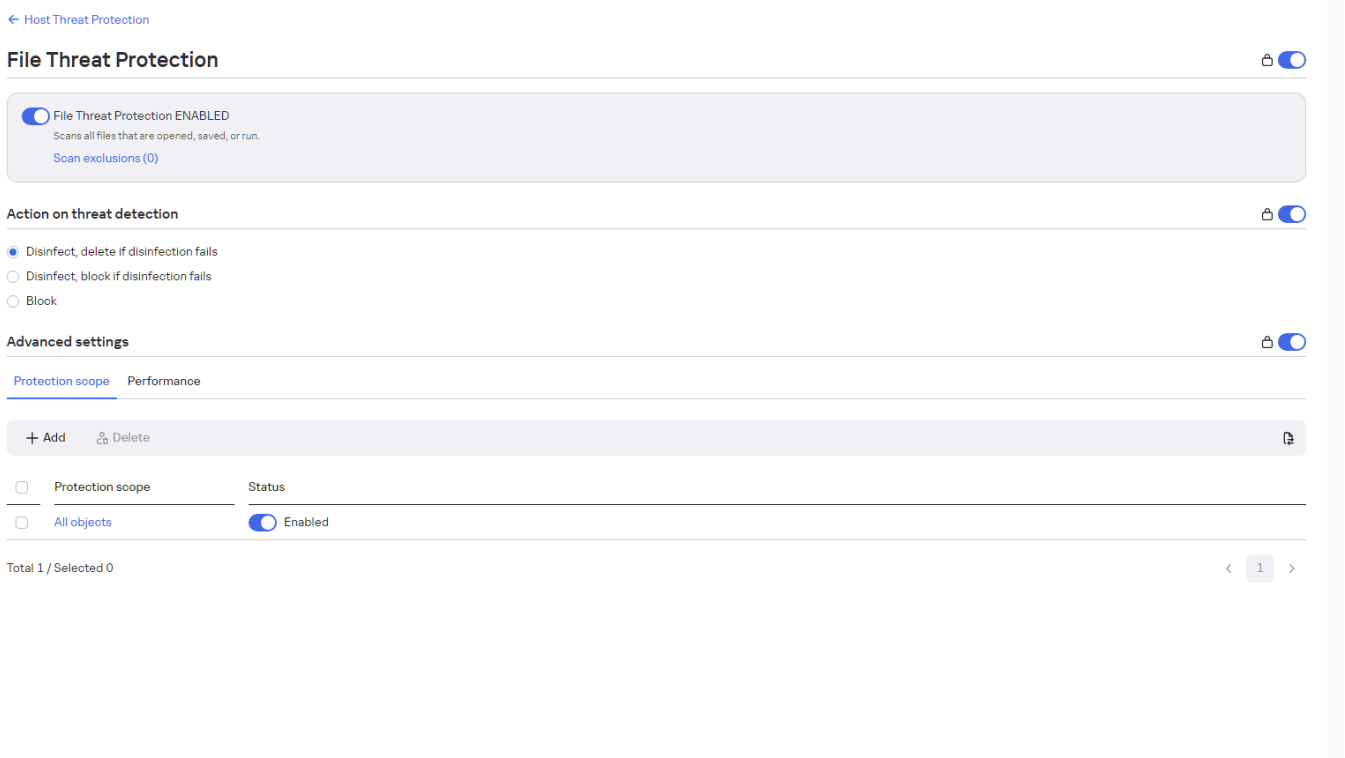
Kaspersky Endpoint Security scans objects in the order they appear in the list of objects. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

How to create a protection scope in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **File Threat Protection**.
5. In the **Protection scope** block, click **Add**.
6. This opens a window; in that window, select the type of file system:
   - **Local**. Directories on the hard drive accessible without a network connection.
   - **Mounted**. Mounted remote or local directories.
   - **Shared**. Computer directories accessible via the Samba (SMB) or NFS protocol.
   - **All remote mounted**. All remote directories mounted on the device using the Samba and NFS protocols.
   - **All shared**. All computer directories accessed via the Samba and NFS protocols.
7. For a local file system, specify a directory path (for example, `/path/to/folder`). If necessary, select the **Include subfolders** check box.
8. Specify the access protocol for a mounted or shared file system.
9. Specify masks for object extensions (for example, `*.txt`). Separate masks with commas.

10. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



File Threat Protection

How to create a protection scope on the command line

1. Run the following command:

```
kesl-control --set-settings 1 --add-path <path>
```

A new `[ScanScope.item_#]` section will be added to the task settings. The application scans the objects in the directory specified by the `Path` setting.

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 1
```

Example

```
kesl-control --set-settings 1 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

The following protection scope settings are added to the task:

```
[ScanScope.item_0001]
AreaDesc=All object
UseScanArea=Yes
Path=/home
AreaMask.item_0000=*
```

How to select an action on file threat detection

Upon detecting malware, Kaspersky Endpoint Security may remove the infected file and terminate the malware process started from this file. In File Threat Protection settings, you can select the action that Kaspersky Endpoint Security performs when a threat is detected.

How to configure the action on threat detection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **File Threat Protection**.
5. Under **Action on threat detection**, select the action that the application will take when a threat is detected:
   - **Disinfect, delete if disinfection fails** (default). If this option is selected, the application automatically attempts to disinfect infected file that is detected. If disinfection fails, the application deletes the file.
   - **Disinfect, block if disinfection fails**. If this option is selected, the application automatically attempts to disinfect infected file that is detected. If disinfection fails, the application blocks this file.
   - **Block**. If this option is selected, the application automatically blocks the infected file without attempting to disinfect or delete it.
6. To apply the policy to computers, close the padlock icons and save your changes.

How to configure the action on threat detection on the command line

1. Run the following command:

```
kesl-control --set-settings 1 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 1
```

Symbols

Command options

Setting	Description
`ActionOnThreat`	Action on threat detection: • `DisinfectDeleteIfNotPossible` (default). If this option is selected, the application automatically attempts to disinfect infected file that is detected. If disinfection fails, the application deletes the file. • `DisinfectBlockIfNotPossible`. If this option is selected, the application automatically attempts to disinfect infected file that is detected. If disinfection fails, the application blocks this file. • `Block`. If this option is selected, the application automatically blocks the infected file without attempting to disinfect or delete it.

What is the Smart mode of file scanning

File Threat Protection scans all files that are opened, saved, or executed. By default, File Threat Protection scans files in smart mode. In *Smart mode*, File Threat Protection scans a file when an attempt is made to open it. If a process repeatedly accesses a file over a period of time and modifies it, File Threat Protection will only rescan the file when that process closes it. This minimizes the impact of the application on system performance while providing a high level of protection.

For the Smart mode to work, the updatable kernel module must be selected and launched.

You cannot change the file scan mode in the Web Console.

How to select the file scan mode on the command line

1. Run the following command:

```
kesl-control --set-settings 1 ScanByAccessType=<SmartCheck|OpenAndModify|Open>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 1
```

Symbols

Command options

Setting	Description
`ScanByAccessType`	File scan mode: • `SmartCheck` (default value). File Threat Protection scans files in smart mode. Kaspersky Endpoint Security scans a file when it is opened and when it is closed, if the file has been modified. If Smart mode is not available, the application scans files when they are opened and every time the file is modified (`OpenAndModify`). Smart mode may not be available, for example, if the updatable kernel module is stopped. • `OpenAndModify`. Kaspersky Endpoint Security scans a file when it is opened and every time the file is modified, not just when it is closed. • `Open`. Kaspersky Endpoint Security scans a file when an attempt is made to open it for reading, execution, or modification.

How to optimize file scanning

Configure file scanning to optimize the File Threat Protection component. This helps reduce CPU utilization on the protected device. You can limit the scanning of archives, set the maximum size of objects that can be scanned, and set the maximum object scan duration.

How to configure file scanning in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **File Threat Protection**.
5. Under **Advanced settings**, select the **Performance** tab and configure file scanning:
   - **Scan archives**. This includes the scanning of ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE and other types of archives. The application identifies archives not just by extension, but also by format. When scanning archives, the application performs recursive unpacking. This makes it possible to detect threats in nested archives (archive inside an archive). The scan is disabled by default.
   - **Scan distribution packages & self-extracting archives**. Scanning installation packages of third-party applications and self-extracting archives. Self-extracting archives are archives that contain an executable extraction module. The scan is disabled by default.
   - **Scan email databases**. Scanning email databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail clients. The scan is disabled by default.
   - **Scan email format files**. Scan plain text email messages. The scan is disabled by default.
   - **Do not scan archives larger than (MB)**. Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.
   - **Skip file that is scanned for longer than (sec)**. Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting. By default, the application tries to scan an object within one minute.
6. To apply the policy to computers, close the padlock icons and save your changes.

How to configure file scanning on the command line

1. Run the following command:

```
kesl-control --set-settings 1 ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<Object size (MB)>
TimeLimit=<Scan time (sec)>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 1
```

Symbols

Setting	Description
`ScanArchived`	This includes the scanning of ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE and other types of archives. The application identifies archives not just by extension, but also by format. When scanning archives, the application performs recursive unpacking. This makes it possible to detect threats in nested archives (archive inside an archive). The scan is disabled by default.
`ScanSfxArchived`	Scanning installation packages of third-party applications and self-extracting archives. Self-extracting archives are archives that contain an executable extraction module. The scan is disabled by default.
`ScanMailBases`	Scanning email databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail clients. The scan is disabled by default.
`ScanPlainMail`	Scan plain text email messages. The scan is disabled by default.
`SkipPlainTextFiles`	Temporary exclusion of files in text format from scans. The application does not scan text files if they are reused by the same process within 10 minutes after the most recent scan. By default, exclusion from scanning is disabled. This setting is intended for devices that support the fanotify mechanism of system events interception. On devices with the updatable kernel module, the application uses the scan result cache to optimize the load.
`SkipDatabaseJournals`	Temporarily excluding database journal files from scanning. The application does not scan database journal files if the journal file is reused by the same process within 10 minutes after the most recent scan. By default, exclusion from scanning is disabled. This setting is intended for devices that support the fanotify mechanism of system events interception. On devices with the updatable kernel module, the application uses the scan result cache to optimize the load.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object. (Value `0`).
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting. By default, the application tries to scan an object within one minute. (Value `60`).

Special considerations for scanning symbolic links and hard links

Kaspersky Endpoint Security lets you scan symbolic links and hard links to files.

A *symbolic link* (also known as a Soft link) is a file that points to another file or directory. A symbolic link and the file it points to can be on different file systems. Also, such a link may point to a file that does not exist. When you delete the target file, the link is not deleted, but it stops working.

A *Hard link* is essentially an alternative name for the file. A hard link points to the index descriptor (inode) of the file that contains the metadata of the file. As long as at least one hard link to the file remains, the file continues to exist in the file system.

Scanning symbolic links

The application scans symbolic links only if the file to which the symbolic link points is within the protection scope of File Threat Protection.

If the file is outside the protection scope, the application does not follow the symbolic link to scan the contents of the file. However, if the file contains malicious code, the security of the device is at risk.

Scanning hard links

If malicious code is detected in a file with more than one hard link pointing to it, the application disinfects the original file. If disinfection proves impossible, the application deletes the hard link and creates in its place a copy of the source file with the name of the deleted link in Backup. The application deletes only the hard link that is being processed, the rest of the hard links that may point to the same data remain intact.

When you restore a hard link from Backup, the application creates a copy of the original file with the name of the hard link being restored in the original location. The restored link does not become a hard link to the original file and remains independent from the other hard links to the same file.

Resolving symbolic links in exclusions by process

If the path in the `ProgramPath` parameter of the `ExcludedForProgram` section is a symbolic link to a binary executable file, the application applies the exclusion to the path of the target file. This rule applies to all links to this file, not just the one explicitly specified. This parameter uses the path to the program image, so symbolic links to scripts (for example, `.sh`) are not resolved.

The target file is determined when the task is run and the settings are applied. If a link points to a nonexistent file, the path to the link itself is included in the exclusions. If the link is replaced with a regular executable file with the same name, the exclusion will apply to that file.

Example of an exclusions with a symbolic link

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/md5sum
UseExcludedForProgram=Yes
Path=/root/s1
```

At the time the task is launched, the `/usr/bin/md5sum` link points to `/bin/coreutils`, so `/bin/coreutils` will be added to the exclusions. If the link is later redirected to `/bin/false`, the exclusion will remain on `/bin/coreutils` until the task is restarted, and will not be applied to `/bin/false`. After the task is restarted, the exclusion will apply to `/bin/false` instead of `/bin/coreutils`.

Malware Scan

Malware scan is vital to computer security. Regularly run malware scans to rule out the possibility of spreading malware that is undetected by protection components due to a low security level setting or for other reasons.

Kaspersky Endpoint Security has the *Malware scan* standard task predefined. You can use this task to perform a full scan of the device. During a full scan, the application scans all objects located on the device's local drives, as well as all mounted and shared objects that are accessed via Samba or NFS protocols with the recommended security settings.

The Administration Server Initial Configuration Wizard automatically creates a *Malware scan* task. To create a *Malware scan* task, install the Kaspersky Endpoint Security for Linux Management Plug-in while running the Wizard. If necessary, you can create user tasks of the *Malware scan* type.

Malware scan task settings

1. **Configure the task run schedule**

   During the scan, Kaspersky Endpoint Security may use more computer resources than usual. We recommend scheduling scan tasks at times when the computer is least loaded.

2. **Optimize the load on the system imposed by the scan**

   You can limit CPU usage when running the Malware Scan task. This may increase the time it takes to scan your computer.

   Kaspersky Endpoint Security allows canceling scheduled tasks when a laptop is running on battery power.

3. **Configure the Malware Scan task settings**

   By default, the Malware Scan task uses the settings recommended by Kaspersky experts. Default settings provide recommended protection level and optimal resource use. If you have special requirements for infrastructure security, you can change these settings.

   By default, the application scans archives. To do this, the application unpacks the archives into the /tmp directory. Make sure there is enough free space on the computer to unpack the archives.

4. **Configure the scan scope**

   By default, the application scans all files on a protected device. If you only need to scan an individual directory (for example, the directory into which files are automatically downloaded from an external source), you can specify only that directory as the scan scope. In other cases, we recommend keeping the default scan scope and using exclusions to fine-tune the scope.

   To scan servers, we recommend dividing the scan scope into several sub-scopes and creating a separate Malware Scan task for each such sub-scope. To spread the load, schedule a different start time for each task.

5. **Add scan exclusions**

   Set up an exclusion scope:

   - **Scan exclusions**. Exclusions help balance system security with performance. For stable operation of third-party software, add to exclusions files and directories which are listed in the documentation for the respective software.

     If you have already created an exclusion scope for the File Threat Protection component, you can also apply these exclusions to the Malware Scan task.

   - **Global exclusions**. Excluding mount points (global exclusions) allows you to refrain from intercepting file operations in certain directories. Exclude shared network resources from the scan scope. To protect shared network resources, use the Kaspersky Endpoint Security application on the device where the resources are physically stored.

6. **Run the Malware Scan task**

   How to run the Malware Scan task in the Web Console

   1. In the main window of the Web Console, select **Tasks**.

      The list of tasks opens.

2. Click the *Malware scan* task of Kaspersky Endpoint Security.

   The task properties window opens.

   The *Malware scan* task is created automatically by the Administration Server quick start wizard. To create a *Malware scan* task, install the Kaspersky Endpoint Security for Linux Management Plug-in while running the Wizard.

   If necessary, you can create user tasks of the *Malware scan* type.

3. On the **Settings** tab, manage the task settings.

4. On the **Application settings** tab, configure the advanced settings of the application (see the table below).

5. On the **Schedule** tab, configure how you want to start the task.

   By default, Kaspersky Endpoint Security is configured to run the task manually.

6. Save your changes.

7. Run the task.

Malware scan task settings

Setting	Description
Scan scope	The table that contains the scopes scanned by the task. By default, only one scan scope is active; it includes all directories of the local file system. You can add scan scopes manually.
Action on threat detection	• **Disinfect, delete if disinfection fails** (default value). If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. • **Disinfect, inform if disinfection fails**. If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. • **Inform**. If you select this action, the application creates a record about the infected object in the log.
Scan archives	If this option is enabled, the application scans archives. The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used. To scan an archive, the application has to unpack it first, which may slow down scanning. You can reduce the duration of archive scans by specifying the **Skip file that is scanned for longer than (sec)** and **Do not scan files larger than (MB)** settings. This option is disabled by default.
Scan distribution packages & self-extracting archives	If this option is enabled, the application scans self-extracting archives. Self-extracting archives are the archives that contain an executable extraction module. This option is disabled by default.
Scan email format files	If this option is enabled, the application scans email messages in text format. The function is disabled by default.
Scan email databases	If this option is enabled, the application scans mail databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail applications. The function is disabled by default.
Do not scan files larger than (MB)	You can specify the maximum size of a file that can be scanned, in megabytes. Possible values: 1–999999. This limitation is disabled by default.
Skip file that is scanned for longer than (sec)	You can specify the maximum scan duration for a file, in seconds. After the specified time, the application stops scanning the file. Possible values: 1–9999. This limitation is disabled by default.

Setting	Description
Do not run multiple scan tasks at the same time	Postponed start of scan tasks if a scan is already running. Kaspersky Endpoint Security will enqueue new scan tasks if the current scan continues. This helps optimize the load on the computer. For example, let's assume that the application has started a Full Scan task according to the schedule. If a user attempts to start a quick scan from the application interface, Kaspersky Endpoint Security will enqueue this quick scan task and then automatically start this task after the Full Scan task is finished. The function is disabled by default.
Use iChecker technology	If this option is enabled, the application scans only new files and files modified after the last scan. If this option is disabled, the application scans files regardless of their creation or modification dates. This option is disabled by default.

How to run the Malware Scan task on the command line

1. By default, the application has the *Malware Scan* (*Scan_My_Computer*) task. If you want to create a new *Malware Scan* task, run the following command:

   ```
   kesl-control --create-task <task name> --type ODS
   ```

   where `<task name>` is the name that you want to set for the new task.

   This command returns the ID of the created task.

2. If necessary, change task settings (see the table below) using the following command:

   ```
   kesl-control --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
   ```

   Example of changing the task settings

   ```
   kesl-control --set-settings 101 ScanFiles=No
   ```

   You can also manage task settings using a configuration file.

3. If necessary, configure a schedule for the task. By default, the task is started manually.

4. To check the current values of the task settings, run the following command:

   ```
   kesl-control --get-settings <task ID|name>
   ```

5. To run the *Malware Scan* task, run the following command:

   ```
   kesl-control --start-task <task ID|name> [-W] [--progress]
   ```

   Command examples

   ```
   kesl-control --start-task 2 -W
   ```

6. To stop the *Malware Scan* task, run the following command:

   ```
   kesl-control --stop-task <task ID|name> [-W]
   ```

Symbols

Malware Scan task settings

Setting	Description	Values
`ScanFiles`	Enables file scan.	`Yes` (default value) — Scan files. `No` — Do not scan files.
`ScanBootSectors`	Enables boot sector scans.	`Yes` (default value) — Scan boot sectors. `No` — Do not scan boot sectors.
`ScanComputerMemory`	Enables process memory and kernel memory scans.	`Yes` (default value) — Scan process memory and kernel memory. `No` — Do not scan process memory and kernel memory.
`ScanStartupObjects`	Enables startup object scans.	`Yes` (default value) — Scan startup objects. `No` — Do not scan startup objects.
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used.	`Yes` (default value) — Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` (default value) — Scan self-extracting archives. `No` — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 0.
`QueueScanTasks`	Delay scheduled scan tasks if a previously started scheduled scan is still running. Kaspersky Endpoint Security will enqueue scheduled scan tasks if the current scan continues. This helps optimize the load on the computer. For example, a scan task is scheduled to run at 6:00 PM and at 8:00 PM. The scan task that is scheduled to run at 8:00 PM is delayed if the 6:00 PM scan is still running. The delayed task is run after the 6:00 PM task finishes.	`Yes` to enqueue scheduled scan tasks if the current scan is still running. `No` (default value) to run scheduled scan tasks even if the current scan is still running.

Setting	Description	Values
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectInformIfNotPossible` (disinfect; inform if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. `Inform` means the application does not try to disinfect or delete the infected object. Information about the infected object is logged. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the scan.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.
	Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled.
		The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Enables exclusion of objects containing the threats specified by the `ExcludeThreats.item_#` setting from scans.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		Example
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Enables global exclusions for scanning.	`Yes` (default value) — Use the global exclusions. `No` — Do not use global exclusions.
`UseOASExclusions`	Enables File Threat Protection exclusions for scanning.	`Yes` (default value) — Use File Threat Protection exclusions. `No` — do not use File Threat Protection exclusions.

Setting	Description	Values
`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) — Do not log information about non-infected objects.
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) — Do not log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) — Do not log information about unprocessed objects.
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts.	`Yes` (default value) — Enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. You can specify the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) — The recommended value.
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) — Enable use of the iChecker technology. `No` — Disable use of the iChecker technology.
`DeviceNameMasks.item_#`	List of device names. The application will scan boot sectors of these devices. The setting value cannot be empty. At least one device name mask must be specified to run this task.	`AllObjects` – scan boot sectors of all devices. `<device name mask>` – Scan boot sectors of the devices whose names match the specified mask. Default value: `/**` – any set of characters in the device name, including the `/` character.
The **[ScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan scope, which contains additional information about the scan scope. The maximum length of the string specified using this setting is 4096 characters.	Default value: `All objects`. Example `AreaDesc="Mail bases scan"`
`UseScanArea`	Enables scans of the specified scope. To run the task, enable scans of at least one scope.	`Yes` (default value) — Scan the specified scope. `No` — Do not scan the specified scope.
`AreaMask.item_#`	Scan scope limitation. Within the scan scope, the application scans only the files that are specified using the masks in the shell format. If this setting is not specified, the application scans all the objects in the scan scope. You can specify several values for this setting.	The default value is `*` (scan all objects). Example `AreaMask.item_0000=*doc`

Setting	Description	Values
`Path`	Path to the directory with objects to be scanned.	`<path to local directory>` – Scan objects in the specified directory. The `/` path is specified by default – the application scans all directories of the local file system. `Shared:NFS` — Scan the device file system resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samba protocol. `Mounted:NFS` – Scan the remote directories mounted on a device using the NFS protocol. `Mounted:SMB` – Scan the remote directories mounted on a device using the Samba protocol. `AllRemoteMounted` – Scan all remote directories mounted on the device using the Samba and NFS protocols. `AllShared` – Scan all the device file system resources that are accessible via the Samba and NFS protocols. `<file system type>` – Scan all resources of the specified file system device.
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan exclusion scope, which contains additional information about the exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.
`AreaMask.item_#`	Limitation of scan exclusion scope. In the exclusion scope, the application excludes only the files that are specified using masks in the shell format. If this setting is not specified, the application excludes all the objects in the exclusion scope. You can specify several values for this setting.	Default value: `*` (exclude all objects)

Setting	Description	Values
`Path`	Path to the directory with objects to be excluded.	`<path to local directory>` – Exclude objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path. In order to optimize the operation of scan tasks, it is recommended to add the path with snapshots mounted by the system in the read-only mode to the exclusions for the systems with the btrfs file system and enabled active snapshots. For example, for the systems based on SUSE/OpenSUSE, you can add the following exclusion `/.snapshots/*/snapshot/`. The `/` path is specified by default. The application excludes all directories of the local file system from scan. `Mounted:NFS` – Exclude the remote directories mounted on a device using the NFS protocol from scan. `Mounted:SMB` – Exclude the remote directories mounted on a device using the Samba protocol from scan. `AllRemoteMounted` – Exclude all remote directories mounted on the device using the Samba and NFS protocols from scan. `<file system type>` – Exclude from scanning all resources of the specified file system device. Remote directories are excluded from scanning by the application only if they were mounted before the task was started. Remote directories mounted after the task is started are not excluded from scanning.

How to run the Malware Scan task from the graphical interface

1. Open the main window of the application graphical interface.
2. Click **Scan**.

   The **Scan** window opens.
3. To start a scan task, click the **Start** button under the scan task that you want to start.

   The progress of the running scan task is displayed.
4. To stop a scan task, click the **Stop** button under the scan task that you want to stop.

   The scan task stops, and information about the scanned objects and detected threats is displayed.
5. To view the report on the scan task, click the **Show report** button.

When an infected object is detected or when a scan task is completed, a corresponding notification is displayed.

The **Scan** window also displays the progress and results of temporary boot sector scan tasks (*Scan_Boot_Sectors_{ID}*) and temporary custom file scan tasks (*Scan_File_{ID}*).

7 Collect computer scan statistics

You can use reports to get scan statistics for a computer. Make sure the scan duration is within the acceptable range. Check the detected objects and, if these objects are trusted, add them to exclusions.

Special considerations and limitations

- If the root user does not have access to a remote directory mounted on the device over the NFSv4 protocol, the application will skip this file during the scan.
- While performing scan tasks, Kaspersky Endpoint Security can disinfect and delete files that are protected from modification: files with the 'immutable' and 'append-only' attributes and files in directories with the 'immutable' and 'append-only' attributes. Backup stores copies of these files that were created before disinfection or deletion. You can restore files from backup copies, if necessary. When scan tasks are completed, the 'immutable' and 'append-only' attributes of disinfected files are not preserved.
- If the user or the watchdog service has restarts the application during the malware scan, or if the computer is restarted during the scan, the scan is stopped. The next time you start the malware scan, it starts from scratch.

Useful articles

What to do if your device runs out of free disk space

How to create a scan scope

A *scan scope* is a list of paths to objects that Kaspersky Endpoint Security scans for threats. By default, the application scans all files on a protected device. If you only need to scan an individual directory (for example, the directory into which files are automatically downloaded from an external source), you can specify this directory as the scan scope.

Kaspersky Endpoint Security scans objects in the order they appear in the list of objects. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

When running on operating systems that use the special-purpose parsecfs file system (Astra Linux Special Edition) we recommend adding mounting paths of this file system to exclusions from scanning.

How to create a scan scope in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the scan task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. In the **Scan scope** section, click **Add**.

5. In the **File system, access protocol, and path** drop-down list, select the type of the file system:

   - **Local**. Directories on the hard drive accessible without a network connection.
   - **Mounted**. Mounted remote or local directories.
   - **Shared**. Computer directories accessible via the Samba (SMB) or NFS protocol.
   - **All remote mounted**. All remote directories mounted on the device using the Samba and NFS protocols.
   - **All shared**. All computer directories accessed via the Samba and NFS protocols.

6. For the **Mounted** and **Shared** file system types, select an access protocol:

   - **NFS**. Remote directories mounted on a device using the NFS protocol.
   - **Samba**. Remote directories mounted on a device using the Samba protocol.
   - **Custom**. File system resources on a device with a type other than NFS or Samba (for example, `ext4` or `parsecfs`).

7. Specify the path to the directory or a path mask.

8. If necessary, specify masks for object names (for example, `*.txt` or `report_*`). Separate masks with commas.

9. Click **Add**.

   The new object is added to the scan scope. You can exclude an object from the scan scope without removing it from the list of objects. To do so, disable the toggle switch next to the object.

10. If necessary, enable or disable the predefined objects in the scan scope:

    - **Kernel Memory**. **Memory of running processes**.
    - **Running processes and Startup Objects**.
    - **Disk boot sectors**.
    - **All hard drives**.
    - **All network drives**.

11. To apply the policy to computers, close the padlock icons and save your changes.

How to create a scan scope on the command line

1. Run the following command:

   ```
   kesl-control --set-settings 2 --add-path <path>
   ```

   A new `[ScanScope.item_#]` section will be added to the task settings. The application will scan the objects in the specified directory.

   Example

   ```
   kesl-control --set-settings 2 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
   ```

   The following scan scope settings will be added to the task:

   ```
   [ScanScope.item_0001]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=/home
   AreaMask.item_0000=*
   ```

2. If you want to include resources from a mounted file system of a specific type other than NFS or Samba (for example, `parsecfs`) in the scan scope, specify the file system type in the `Path` parameter: Path=<file system type>

   The application will scan all the resources of the specified device file system.

   Example

   ```
   kesl-control --set-settings 2 ScanScope.item_0002.UseScanArea=Yes ScanScope.item_0002.Path=parsecfs
   ```

   The following scan scope settings will be added to the task:

   ```
   [ScanScope.item_0002]
   AreaDesc=All objects
   UseScanArea=Yes
   Path=parsecfs
   AreaMask.item_0000=*
   ```

3. To check the current values of the task settings, run the following command:

   ```
   kesl-control --get-settings 2
   ```

How to configure a scan schedule

Running the task *Malware Scan* may increase resource utilization on the computer. To minimize the impact of Kaspersky Endpoint Security on the performance of users' computers while they are in active use, you can schedule the task to run at the most opportune time.

For example, if employees in your organization work on a fixed schedule, you can configure the scan to run at night or on weekends. If it is impossible to run the scan for any reason (for example, the computer is off at that time), you can configure the skipped task to be run automatically as soon as this becomes possible.

If you are unable to determine the optimal schedule for running a computer scan, you can run the *Malware Scan* task not only at specific times but also based on specific conditions, such as when an application is launched, when updates are downloaded to the repository, when a virus attack is detected, or when another task is completed. You can also use the Wake-on-LAN functionality to power on computers that are powered off a short time before the task starts. You can configure running the scan using Wake-on-LAN only for the *Malware Scan* task in Kaspersky Security Center. You cannot enable Wake-on-LAN for scanning the computer in the application interface.

How to run the Malware Scan task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the scan task.

   The task properties window opens.

3. In the task properties window, select the **Schedule** tab.

4. Configure the scan task schedule.

5. Depending on the selected frequency, configure advanced settings that specify the task run schedule (see the table below).

6. Save your changes.

Scan schedule settings

Setting	Description
Start task	**Manually**. Run mode in which you can start scan manually at a time when it is convenient for you. By schedule. In this scan task run mode, the application starts the scan task in accordance with the schedule that you create. If this scan task run mode is selected, you can also start the scan task manually.
Run missed tasks	If the check box is selected, Kaspersky Endpoint Security starts the skipped task as soon as it becomes possible. The task may be skipped, for example, if the computer was off at the scheduled task start time. When the application gets an opportunity to execute missed tasks, it runs the tasks randomly within a certain time interval to distribute the load on the computer. If the check box is cleared, Kaspersky Endpoint Security does not run skipped tasks. Instead, it carries out the next task in accordance with the current schedule.
Use automatically randomized delay for task starts	If the check box is selected, the task is not run strictly on schedule, but randomly within a certain interval, that is, the start times of the task are spread out. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. The range of randomized start times is automatically calculated when the task is created, depending on the number of computers that have the task assigned. Subsequently, the task is always run at its calculated start time. However, whenever task settings are modified or the task is run manually, the calculated start time changes. If the check box is cleared, the task is run exactly at scheduled time.
Use automatically randomized delay for task starts within an interval of	If this check box is selected, the task is run on computers at a random time within a certain time frame. Randomized start times help avoid a great number of computers simultaneously accessing the Administration Server when the task is run on schedule. If the check box is cleared, the task is run exactly at scheduled time.
Turn on devices by using the Wake-on-LAN function before starting the task	If the check box is selected, the operating system of the computer is given a specified lead time to complete startup before the task is run. The default lead time is 5 minutes. Select the check box if you want to run the task on all computers including powered off computers.
Shut down the devices after completing the task	If this check box is selected, the computer will shut down after the task is completed. For example, you can enable this functionality to scan the computer on Fridays after working hours. When the task finishes, the application turns off the computer for the weekend.
Stop the task if it runs longer than	Limiting the task execution time. After the specified amount of time, Kaspersky Endpoint Security stops the task. The task is not marked as completed. Next time Kaspersky Endpoint Security runs the task, it will be run from the beginning and on schedule.

How to schedule the Malware Scan task on the command line

To run the task once at a specific time, run the following command:

```
kesl-control --set-schedule 2 RuleType=Once StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>'
```

To run the task monthly, run the following command:

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='<hh>:<mm>:<ss>;<day of the month>'
```

To run the task on a specific day of the week, run the following command:

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='<hh>:<mm>:<ss>;<day of the week>'
```

To run the task at regular intervals in days, run the following command:

```
kesl-control --set-schedule 2 RuleType=Daily StartTime='<hh>:<mm>:<ss>;<interval between runs (in days)>'
```

To run the task at regular intervals in hours starting from a specific date, run the following command:

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='<year>/<month>/<day of the month> <hh>:<mm>:<ss>;
<interval between runs (in hours)>'
```

To run the task at regular intervals starting from a specific date, run the following command:

```
kesl-control --set-schedule 2 RuleType=Minutely StartTime='<hh>:<mm>:<ss>;<interval between runs (in minutes)>'
```

To run the task immediately after the application starts, run the following command:

```
kesl-control --set-schedule 2 RuleType=PS
```

To run the task immediately after databases are updated, run the following command:

```
kesl-control --set-schedule 2 RuleType=BR
```

To disable scheduling for the task, run the following command:

```
kesl-control --set-schedule 2 RuleType=Manual
```

To manage additional task schedule settings, run the following command:

```
kesl-control --set-schedule 2 RandomInterval=<time interval (minutes)> RunMissedStartRules=<Yes|No>
UseWorkingTimeout=<Yes|No> WorkingTimeout=<maximum task completion time (minutes)> QueueScanTasks=<Yes|No>
```

To check the current values of the task settings, run the following command:

```
kesl-control --get-schedule 2
```

Symbols

Task start schedule settings

Setting	Description
`RuleType`	Task launch schedule. • `Once`: run the task once. • `Monthly`: run the task on the specified day and time every month. • `Weekly`: run the task on the specified day and time every week. • `Daily`: run the task regularly, at the specified interval in days. • `Hourly`: run the task regularly, at the specified interval in hours, starting on the specified date and time. • `Minutely`: run the task regularly, at the specified interval in minutes, starting at the specified time. • `Manual` – start the task manually. • `PS` – start the task after starting the application. • `BR` – start the task after the application databases have been updated.
`StartTime`	Task start date and time. The format of this setting depends on the `RuleType`. Possible values: • `<year>`: 1970 to 2099 • `<month>`: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. • `<day of the month>`: 1 to 31 • `<day of the week>`: Mon, Tue, Wed, Thu, Fri, Sat, Sun. • `<hh>`: 0 to 23 • `<mm>`: 0 to 59 • `<ss>`: 0 to 59 • `<interval between runs (in days)>`: 0 to 364 • `<interval between runs (in hours)>`: 0 to 23 • `<interval between runs (in minutes)>`: 0 to 59
`RandomInterval`	Run the task on computers randomly within a certain time interval (from 0 to the specified value). This avoids multiple tasks starting at the same time. Default value: 99 minutes. Possible values: 0 – 999.
`RunMissedStartRules`	Runs a missed task after the application is started. • `Yes` (default value) means that running a missed task is enabled. If the application is stopped or the computer is powered off while a scheduled task is running, Kaspersky Endpoint Security starts that task immediately after the application starts. This helps you make sure critical tasks are never missed. • `No` means that running a missed task is disabled. If the application is stopped or the computer is powered off while a scheduled task is running, the application skips that task. This helps you avoid extra load when starting the application.
`UseWorkingTimeout`	Stops the task upon reaching the maximum task execution time specified by the `WorkingTimeout` setting. The task will be stopped even if it is not completed. The next launch of the task will be performed according to the schedule. • `Yes` – Stop the task when the maximum task execution time has been reached. • `No` (default value) – Do not stop the task when the maximum task execution time has been reached.
`WorkingTimeout`	The maximum task execution time (in minutes) after which the application stops executing the task if `UseWorkingTimeout=Yes`. Default value: 120 minutes. Possible values: 1 – 999.

Example of running the scan task every 10 hours

```
kesl-control --set-schedule 2 RuleType=Hourly StartTime='2030/May/28 12:00:00;10'
```

Example of running the scan task on the 15th of each month

```
kesl-control --set-schedule 2 RuleType=Monthly StartTime='12:00:00;15'
```

Example of running the task every Tuesday

```
kesl-control --set-schedule 2 RuleType=Weekly StartTime='12:00:00;Tue'
```

How to scan an individual file or directory

Kaspersky Endpoint Security lets you run a scan of individual files for viruses and other malware using the command line. For example, you can selectively scan archives for which File Threat Protection scanning is disabled by default.

By default, the application scans the file using the *Scan_File (ID: 3)* task settings recommended by Kaspersky experts. Default settings provide the recommended protection level and optimal resource use. By default, the application saves a copy of an infected object in Backup and tries to disinfect the object. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. You can select a different action on threat detection and manage other task settings.

How to start scanning an individual file or directory on the command line

```
kesl-control --scan-file <path to the file or directory>
```

As a result, Kaspersky Endpoint Security generates a report of the following form:

```
Scanned objects: N

Total detected objects: N

Infected objects and other objects: N

Disinfected objects: N

Moved to Backup: N

Removed objects: N

Non-disinfected objects: N

Scan errors: N

Password-protected objects: N

Skipped objects: N

Detected by Cloud Sandbox: N
```

How to optimize custom scan tasks

To optimize custom scans, you can limit the simultaneous launch of multiple tasks. If a user tries to run too many custom scan tasks at the same time, the application will not run the tasks that exceed the limit. This allows you to control the utilization of resources of the client device and, for example, avoid excessive load on the server. By default, the limit on the number of custom scan tasks is set to 100.

Kaspersky Endpoint Security limits tasks only for unprivileged users. A user with root privileges can run custom scan tasks without limitations.

You can configure the custom scan task limit on the command line using general application settings. You cannot configure the task limit in the Administration Console or the Web Console.

How to optimize custom scan tasks on the command line

```
kesl-control --set-app-settings LimitNumberOfScanFileTasks=<number of tasks>
```

Critical Areas Scan

A special scan task lets you scan only critical areas of the computer: *Critical Areas Scan*. The *Critical Areas Scan* quickly scans the areas of the computer in which malware is found most often. The scan scope of this task includes boot sectors, startup objects, kernel memory, and running processes.

Malware that manages to compromise critical areas of the computer can realize its functionality while evading detection. By default, the application runs the task with settings recommended by Kaspersky experts. Default settings provide the recommended protection level and optimal resource use.

Kaspersky experts do not recommend changing the default settings of the *Critical Areas Scan* task.

If the root user does not have access to a remote directory mounted on the device over the NFSv4 protocol, the application will skip this file during the scan.

The Administration Server Initial Configuration Wizard automatically creates a *Critical Areas Scan* task. To create a *Critical Areas Scan* task, install the Kaspersky Endpoint Security for Linux Management Plug-in while running the Wizard. If necessary, you can create user tasks of the *Critical Areas Scan* type.

How to run a critical areas scan in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux**.

   b. In the **Task type** drop-down list, select **Critical Areas Scan**.

   c. In the **Task name** field, enter a brief description, for example, *Critical Areas Scan after a computer infection*.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option. Proceed to the next step.

5. Finish the wizard.

6. Click the scan task.

   The task properties window opens.

7. Select the **Application settings** tab.

8. Configure the scan task (see the table below).

9. If necessary, configure the task start schedule settings on the **Schedule** tab.

10. Save your changes.

11. Run the scan task.

Critical Areas Scan task settings

Setting	Description
Scan scope	The table that contains the scopes scanned by the task. By default, the scan scope includes all directories of the local file system, kernel memory, memory of running processes, startup objects, and boot sectors.
Action on threat detection	• **Disinfect, delete if disinfection fails** (default). If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. • **Disinfect, inform if disinfection fails**. If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. • **Inform**. If you select this action, the application creates a record about the infected object in the log.
Scan archives	If this option is enabled, the application scans archives. The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used. To scan an archive, the application has to unpack it first, which may slow down scanning. You can reduce the duration of archive scans by specifying the **Skip file that is scanned for longer than (sec)** and **Do not scan files larger than (MB)** settings. This option is disabled by default.
Scan distribution packages & self-extracting archives	If this option is enabled, the application scans self-extracting archives. Self-extracting archives are the archives that contain an executable extraction module. This option is disabled by default.
Scan email format files	Scan plain text email messages. The function is disabled by default.
Scan email databases	If this option is enabled, the application scans mail databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail applications. The function is disabled by default.
Do not scan files larger than (MB)	You can specify the maximum size of a file that can be scanned, in megabytes. Possible values: 0–9999. If the value is set to 0, the application scans files of any size. The function is disabled by default.
Skip file that is scanned for longer than (sec)	You can specify the maximum scan duration for a file, in seconds. After the specified time, the application stops scanning the file. Possible values: 0–9999. If the value is set to 0, the scan time is unlimited. The function is disabled by default.
Do not run multiple scan tasks at the same time	Postponed start of scan tasks if a scan is already running. Kaspersky Endpoint Security will enqueue new scan tasks if the current scan continues. This helps optimize the load on the computer. For example, let's assume that the application has started a Full Scan task according to the schedule. If a user attempts to start a quick scan from the application interface, Kaspersky Endpoint Security will enqueue this quick scan task and then automatically start this task after the Full Scan task is finished. The function is disabled by default.
Use iChecker technology	If this option is enabled, the application scans only new files and files modified after the last scan. If this option is disabled, the application scans files regardless of their creation or modification dates. This option is disabled by default.

How to run the Critical Areas Scan task on the command line

1. If necessary, configure the task settings (see the table below).

```
kesl-control --set-settings 4 <setting name>=<setting value>
```

2. If necessary, configure the task schedule.

3. To check the current values of the task settings, run the following command:

```
kesl-control --get-settings 4 [--json]
```

where `--json` means output data in JSON format.

4. To run the task, run the following command:

```
kesl-control --start-task 4 [-W] [--progress]
```

Where:

- `[-W]` enables the output of current events related to the task.
- `[--progress]`: display task progress.

If necessary, you can create user tasks of the *Critical Areas Scan* type.

Critical Areas Scan task settings

Setting	Description	Values
`ScanFiles`	Enables file scan.	`Yes` — Scan files. `No` (default value) — Do not scan files.
`ScanBootSectors`	Enables boot sector scans.	`Yes` (default value) — Scan boot sectors. `No` — Do not scan boot sectors.
`ScanComputerMemory`	Enables process memory and kernel memory scans.	`Yes` (default value) — Scan process memory and kernel memory. `No` — Do not scan process memory and kernel memory.
`ScanStartupObjects`	Enables startup object scans.	`Yes` (default value) — Scan startup objects. `No` — Do not scan startup objects.
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used.	`Yes` (default value) — Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` (default value) — Scan self-extracting archives. `No` — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.

Setting	Description	Values
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 0.
`QueueScanTasks`	Delay scheduled scan tasks if a previously started scheduled scan is still running. Kaspersky Endpoint Security will enqueue scheduled scan tasks if the current scan continues. This helps optimize the load on the computer. For example, a scan task is scheduled to run at 6:00 PM and at 8:00 PM. The scan task that is scheduled to run at 8:00 PM is delayed if the 6:00 PM scan is still running. The delayed task is run after the 6:00 PM task finishes.	`Yes` to enqueue scheduled scan tasks if the current scan is still running. `No` (default value) to run scheduled scan tasks even if the current scan is still running.
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectInformIfNotPossible` (disinfect; inform if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. `Inform` means the application does not try to disinfect or delete the infected object. Information about the infected object is logged. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the scan.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.
	Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled.
		The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Enables exclusion of objects containing the threats specified by the `ExcludeThreats.item_#` setting from scans.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

Setting	Description	Values

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		`Example`
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Enables global exclusions for scanning.	`Yes` (default value) — Use the global exclusions. `No` — Do not use global exclusions.
`UseOASExclusions`	Enables File Threat Protection exclusions for scanning.	`Yes` (default value) — Use File Threat Protection exclusions. `No` — do not use File Threat Protection exclusions.
`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) — Do not log information about non-infected objects.
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) — Do not log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) — Do not log information about unprocessed objects.
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts.	`Yes` (default value) — Enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. You can specify the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) — The recommended value.
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) — Enable use of the iChecker technology. `No` — Disable use of the iChecker technology.
`DeviceNameMasks.item_#`	List of device names. The application will scan boot sectors of these devices. The setting value cannot be empty. At least one device name mask must be specified to run this task.	`AllObjects` – scan boot sectors of all devices. `<device name mask>` – Scan boot sectors of the devices whose names match the specified mask. Default value: `/**` – any set of characters in the device name, including the `/` character.
The `[ScanScope.item_#]` section contains the following settings:		

Setting	Description	Values
`AreaDesc`	Description of the scan scope, which contains additional information about the scan scope. The maximum length of the string specified using this setting is 4096 characters.	Default value: `All objects`. Example `AreaDesc="Mail bases scan"`
`UseScanArea`	Enables scans of the specified scope. To run the task, enable scans of at least one scope.	`Yes` (default value) — Scan the specified scope. `No` — Do not scan the specified scope.
`AreaMask.item_#`	Scan scope limitation. Within the scan scope, the application scans only the files that are specified using the masks in the shell format. If this setting is not specified, the application scans all the objects in the scan scope. You can specify several values for this setting.	The default value is `*` (scan all objects). Example `AreaMask.item_<item number>=*doc`
`Path`	Path to the directory with objects to be scanned.	`<path to local directory>` – Scan objects in the specified directory. The `/` path is specified by default – the application scans all directories of the local file system. `Shared:NFS` — Scan the device file system resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samba protocol. `Mounted:NFS` – Scan the remote directories mounted on a device using the NFS protocol. `Mounted:SMB` – Scan the remote directories mounted on a device using the Samba protocol. `AllRemoteMounted` – Scan all remote directories mounted on the device using the Samba and NFS protocols. `AllShared` – Scan all the device file system resources that are accessible via the Samba and NFS protocols. `<file system type>` – Scan all resources of the specified file system device.
The `[ExcludedFromScanScope.item_#]` section contains the following settings:		
`AreaDesc`	Description of the scan exclusion scope, which contains additional information about the exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.
`AreaMask.item_#`	Limitation of scan exclusion scope. In the exclusion scope, the application excludes only the files that are specified using masks in the shell format. If this setting is not specified, the application excludes all the objects in the exclusion scope. You can specify several values for this setting.	Default value: `*` (exclude all objects)

Setting	Description	Values
`Path`	Path to the directory with objects to be excluded.	`<path to local directory>` – Exclude objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path. In order to optimize the operation of scan tasks, it is recommended to add the path with snapshots mounted by the system in the read-only mode to the exclusions for the systems with the btrfs file system and enabled active snapshots. For example, for the systems based on SUSE/OpenSUSE, you can add the following exclusion `/.snapshots/*/snapshot/`. The `/` path is specified by default. The application excludes all directories of the local file system from scan. `Mounted:NFS` – Exclude the remote directories mounted on a device using the NFS protocol from scan. `Mounted:SMB` – Exclude the remote directories mounted on a device using the Samba protocol from scan. `AllRemoteMounted` – Exclude all remote directories mounted on the device using the Samba and NFS protocols from scan. `<file system type>` – Exclude from scanning all resources of the specified file system device. Remote directories are excluded from scanning by the application only if they were mounted before the task was started. Remote directories mounted after the task is started are not excluded from scanning.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Container Scan

Kaspersky Endpoint Security can scan containers and images for malware in real time or on demand.

To use the Container Scan functionality, a license that includes this function is required.

The component is not available for devices with an Elbrus CPU.

Container monitoring

The *Container Monitoring* component scans running containers and namespaces in real time. The Container Monitoring component is enabled by default.

For the Container Monitoring component to work, the File Threat Protection component must be enabled. File Threat Protection settings are applied when scanning containers and namespaces.

The recommended Container Monitoring configuration scenario involves the following steps:

1. **Configure the integration of the application with container management tools**

   The application supports integration with the Docker container management system, the CRI-O environment, and the Podman and runc utilities.

2. **Create a protection scope**

   Determine the devices on which you want to scan containers and namespaces.

3. **In the Container Monitoring settings, select the Skip container action**

   When an infected object is detected in a container, Kaspersky Endpoint Security can immediately stop the container, take no action, or stop the container disinfecting the object or eliminating the threat has proved impossible. Select the **Skip container** action to test the component. The application will not perform any action on the container when an infected object is detected, but will log information about detected threats.

4. **Collect Container Monitoring statistics**

   You can get Container Monitoring statistics using reports.

5. **Select the action to be performed on a container when an infected object is detected.**

   Select the action that the application performs on a container when it detects an infected object.

On-demand scan of containers

The application can scan containers and images for viruses and other malware on demand. This is done using the predefined *Container Scan (Container_Scan)* task. You can configure the predefined task or create user tasks for scanning containers on the command line, in the Web Console, or the Administration Console.

The application can run multiple Container Scan tasks simultaneously.

The recommended Container Scan configuration scenario involves the following steps:

1. **Configure the integration of the application with container management tools**

   The application supports integration with the Docker container management system, the CRI-O environment, and the Podman and runc utilities.

2. **Set up a scan scope**

   By default, the application scans all containers on a protected device. If you need to scan only individual containers, you can specify their names or name masks.

3. **In the Container Scan settings, select the Skip container and Skip image actions**

   When an infected object is detected in a container, Kaspersky Endpoint Security can immediately stop the container, take no action, or stop the container disinfecting the object or eliminating the threat has proved impossible. If an infected object is detected in the container image, Kaspersky Endpoint Security may delete the container image or take no action with the container image. Select the **Skip container** and **Skip image** actions to test the task. The application will not perform any action on the container and the image when an infected object is detected, but will log information about detected threats.

4. **Collect Container Scan statistics**

   You can get Container Scan statistics using reports.

5. **Optimize application performance**

   After analyzing the gathered information, optimize application performance:

   - Add global exclusions
   - Add scan exclusions
   - Optimize Container Scan

6. **Select the action to be performed on a container and its image when an infected object is detected**

   Select the actions that the application performs on a container and its image when it detects an infected object.

Custom Container Scan

The *Custom Container Scan* task allows configuring and storing settings that are used when scanning the specified containers and images using the following command:

```
kesl-control --scan-container
```

A custom scan is performed with the settings stored in the predefined task *Custom_Container_Scan* (ID: 19). You can configure Custom Container Scan settings by editing the settings of this task. By default, the *Custom_Container_Scan* task has the same settings as the *Container_Scan* task (ID:18).

The command creates and runs a temporary task to scan containers and images, which is automatically deleted after completion. In this case, the scan results are output to the console.

Special considerations and limitations

- The application does not scan namespaces and containers unless components for working with containers and namespaces are installed in the operating system. In this case, the component status for Container Monitoring on the command line is displayed as "Task is available and not running", whereas in Kaspersky Security Center, it is displayed as "Stopped".
- A Container Monitoring action can be selected only when the application's license includes this function.

How to configure integration with container management tools

The application supports integration with the Docker container management system, the CRI-O environment, and the Podman and runc utilities. You can configure integration with these container management tools.

How to configure integration with container management tools in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Container Scan settings**.
5. Make sure the toggle switch for the Container Monitoring component is in the **Monitoring of namespaces and containers ENABLED** position.
6. In the **Container Scan settings** block, click the **Configure** button.
7. This opens the **Scan settings** window; in that window, select the boxes next to the container management tools that are installed and used in the operating system of the protected devices, then manage the settings as necessary:
   - The **Use Docker** check box enables the Docker container management system. This check box is selected by default.
     - **Docker socket path** is an entry field for the path or URI (Uniform Resource Identifier) of the Docker socket. Default value: /var/run/docker.sock.
   - The **Use CRI-O** check box enables the CRI-O environment. This check box is selected by default.
     - **File path** is an entry field for the path to CRI-O configuration file. Default value: /etc/crio/crio.conf.

- The **Use Podman** check box enables the Podman utility. This check box is selected by default.
  - **File path** is an entry field for the path to the Podman utility executable file. Default value: /usr/bin/podman.
  - **Root directory** is an entry field for the path to the root directory of the container storage.
- The **Use runc** check box enables the runc utility. This check box is selected by default.
  - **File path** is an entry field for the path to the runc utility executable file. Default value: /usr/bin/runc.
  - **Root directory** is an entry field for the path to the root directory of the container state storage. Default value: /run/runc.

8. Save your changes.

How to configure integration with container management tools on the command line

On the command line, you can enable or disable real-time monitoring of namespaces and containers by using the `NamespaceMonitoring=<Yes|No>` setting from the general application settings.

You can edit the value for the setting `NamespaceMonitoring` using the configuration file that contains all general application settings, or using command line options.

```
Enable monitoring of namespaces and containers using command line options

kesl-control --set-app-settings NamespaceMonitoring=Yes
```

When scanning namespaces and containers in real time, Container Scan settings are applied. You can view and edit these settings using special administration commands for Kaspersky Endpoint Security:

- You can output the current values of Container Scan settings to the console or to a configuration file. You can use this file to edit the settings.
- You can edit all Container Scan settings using the configuration file that contains the settings. You can get the configuration file using the command for displaying general Container Scan settings.
- You can manage individual settings using command line options in the `<setting name>=<setting value>` format. You can get the current values of the settings using a command to output Container Scan settings.

```
Output current values of container scan settings to the console

kesl-control --get-container-settings [--json]
```

Where `--json` is specified to output the settings in JSON format. If the `--json` option is not specified, the settings are output in the INI format.

```
Output current values of container scan settings to a file

kesl-control --get-container-settings --file <path to configuration file> [--json]
```

Where:

- `--file <path to configuration file>` is the path to the file in which you want to save Container Scan settings. If you specify the name of a file without specifying its path, the file will be created in the current directory. If a file with the specified name already exists in the specified path, it will be overwritten. If the specified directory cannot be found on the disk, file will not be created.

- `--json` is specified to output the settings in JSON format. If the `--json` option is not specified, the settings are output in the INI format.

To modify the values of Container Scan settings using a configuration file:

1. Output the Container Scan settings to a configuration file, as described above.

2. Edit the values of the necessary parameters in the file and save the changes.

3. Run the following command:

   ```
   kesl-control --set-container-settings --file <path to configuration file> [--json]
   ```

   Where:

   - `--file <path to configuration file>` is the full path to the configuration file with Container Scan settings.

   - Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

All values of Container Scan settings specified in the file are imported into the application.

```
Modify the values of Container Scan settings using command line options
kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Where `<setting name>=<setting value>` is the name and value of a Container Scan setting.

The values of the specified Container Scan settings are modified.

How to create an on-demand scan scope for containers and images

Scan scope

A *scan scope* is a list of names of containers that Kaspersky Endpoint Security scans while running the *Container Scan* task.

By default, the *Container Scan* task scans all containers on a protected device. If you need to scan only individual containers, you can specify their names or name masks.

How to create a scan scope in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. In the list of tasks, select the Kaspersky Endpoint Security Container Scan task and click the name of the task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Under **Advanced scan settings** → **Container Scan settings**, in the **Name mask** field, enter the name or name mask of the container that you want to scan. By default, all containers are scanned.

5. Under **Advanced scan settings** → **Image scan settings**, in the **Name mask** field, enter the name or name mask of the container image that you want to scan. By default, all images are scanned.

6. Save your changes.

How to create a scan scope on the command line

1. Configure a scan scope using the following command:

   ```
   kesl-control --set-settings <task ID|name> ScanContainers=Yes ContainerNameMask=<container name or mask>
   ScanImages=Yes ImageNameMask=<image name or mask>
   ```

   Where:

   - `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
   - `<container name or mask>` is the name or name mask of the container that you want to scan. Masks are specified in command shell format. You can use the `?` and `*` symbols. By default, all containers are scanned.
   - `<image name or mask>` is the name or name mask of the image that you want to scan. Masks are specified in command shell format. You can use the `?` and `*` symbols. By default, all images are scanned.

2. You can also configure a scan scope using a configuration file:

   a. Output task settings to a configuration file by running the following command:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Open the configuration file for editing.

   c. Add the following settings to the file:

   - `ScanContainers=Yes` enables scanning of the specified containers.
   - `ContainerNameMask=<container name or mask>` is the name or name mask of the container that you want to scan. Masks are specified in command shell format. You can use the `?` and `*` symbols. By default, all containers are scanned.

- `ScanImages=Yes` enables scanning of the specified images.

- `ImageNameMask=<image name or mask>` is the name or name mask of the image that you want to scan. Masks are specified in command shell format. You can use the `?` and `*` symbols. By default, all images are scanned.

```
Example of a container scan performed on a container named my_container
```

```
ContainerNameMask=my_container
```

```
Example of scanning all containers whose names start with my_container
```

```
ContainerNameMask=my_container*
```

```
Example of a container scan performed on all containers whose names start with my_, then contain any five characters, then _container, and end with any characters sequence
```

```
ContainerNameMask=my_?????_container*
```

```
Example of an image scan performed on images with the "my_image" name, and the "latest" tag
```

```
ImageNameMask=my_image:latest
```

```
Example of an image scan performed on all images whose names start with my_image_ and with any tag
```

```
ImageNameMask=my_image*
```

d. Save the changes in the configuration file.

e. Import settings from the configuration file to the task using the following command:

```
kesl- <task ID|name> --file <path> [--json]
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

- `--file <path>` is the full path to the configuration file from which you want to import the task settings.

- Specify the `--json` option if you are importing settings from a JSON configuration file. If the --json option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

All values of the task settings defined in the file will be imported into the application.

Scan exclusions

A *scan exclusion* is a set of conditions that must be fulfilled so that Kaspersky Endpoint Security will not scan a particular object for viruses and other threats. Scan exclusions let you work with legitimate applications that intruders can use to compromise the computer or user data. Such applications do not necessarily have a malicious purpose, but can be exploited by hackers. For detailed information about legitimate applications that intruders can use to compromise the computer or user data, please visit the Kaspersky Encyclopedia website.

You can also exclude certain trusted directories from the scan scope to optimize application performance.

You can exclude objects from scans by using the following methods:

- **Exclusions by mask**. Enter a file name with a mask. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

  Use masks:

  - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and directories in paths to files and directories). For example, the mask `/dir/*/*.txt` will include all paths to files with the TXT extension located in directories within the dir directory, but not in subdirectories.

  - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or directory name, including the `\` and `/` characters (delimiters of the names of files and directories in paths to files and directories). For example, the mask `/dir/**/*.txt` will include all paths to files with the TXT extension located in directories nested within the dir directory, excluding the dir directory itself.

  - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and directories in paths to files and directories). For example, the `/dir/???.txt` mask will include paths to all files residing in the dir directory that have the TXT extension and a name consisting of three characters.

- **Exclusions by threat name** Enter the name of the object type according to the classification of the Kaspersky Encyclopedia (for example, `Email-Worm`, `Rootkit` or `RemoteAdmin`). You can use masks with the `?` character (replaces any single character) and the `*` character (replaces any number of characters). For example, if the `Client*` mask is specified, the application excludes `Client-IRC`, `Client-P2P` and `Client-SMTP` objects from scans.

Kaspersky Endpoint Security also allows excluding from scanning files of certain formats: archives, email databases, text files, database log files.

How to add scan exclusions in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. In the list of tasks, select the Kaspersky Endpoint Security Container Scan task and click the name of the task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Go to the **Exclusion scopes** section.

5. Add exclusions by mask, if necessary:

   a. In the **Exclusions by mask** block, click the **Add** button.

   b. This opens a window; in that window, specify templates for the names of files that you want Kaspersky Endpoint Security to exclude from scanning.

   c. Click **Add**.

   Exclusions are added to the list.

6. Add exclusions by threat name, if necessary:

   a. In the **Exclusions by threat name** block, click the **Add** button.

   b. This opens a window; in that window, specify templates for threat names. The application will not block the specified threats.

   For example, if you use a tool to scan your network, add the full name of its threat to the list of threats to be excluded from scanning.

   You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.

7. If necessary, you can import or export exclusions for each of the lists:

   - To export the list of exclusions, click the **Export** button.

     Kaspersky Endpoint Security saves an export.json file in your standard downloads folder.

   - To import the list of exclusions:

     a. Click **Import**.

     b. Select the JSON file from which you want to import exclusion scopes.

     c. Open the file.

     d. Select the import method: add exclusions to the existing list or replace the list of exclusions.

     e. Save your changes.

     The rules from the JSON file are displayed in the list.

8. Save your changes.

How to add scan exclusions on the command line

1. Add an exclusion scope using the following command:

   ```
   kesl-control --set-settings <task ID|name> --add-exclusion <path>
   ```

   where:

   - `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

   - `--add-exclusion <path>` adds the path to the directory with the objects that you want to exclude from the scan.

   A new `[ExcludedFromScanScope.item_#]` section will be added to the task settings. The application will exclude objects in the directory specified by the `Path` setting from scans. The remaining settings of the exclusion scope take default values.

   If the task settings already contain an `[ExcludedFromScanScope.item_#]` section with the specified value for the `Path` setting, a duplicate section is not added.

   If the `UseScanArea` setting is set to `No` its value will change to `Yes` after this command is executed and the objects located in this directory will be excluded from scans.

2. You can also add an exclusion scope using a configuration file:

   a. Output task settings to a configuration file by running the following command:

   ```
   kesl-control --get-settings <task ID|name> [--json]
   ```

   b. Open the configuration file for editing.

   c. Add an `[ExcludedFromScanScope.item_#]` section to the file with the following settings:

   - `AreaDesc` – a description of the exclusion scope, which contains additional information about the exclusion scope.
   - `UseScanArea` enables exclusion of the specified scope.
   - `Path` is a path to the directory with the objects to be excluded. You can specify a path to a local directory or exclude remote directories mounted on a client device. Possible values for the setting depend on the type of task.
   - `AreaMask.item_#` is a limitation of the exclusion scope. You can specify a mask for the name of the files that you want to exclude from the scan scope. By default, all objects in the scope are excluded.

     Example

     ```
     [ExcludedFromScanScope.item_0000]
     AreaDesc=
     UseScanArea=Yes
     Path=/tmp/notchecked
     AreaMask.item_0000=*
     ```

   d. You can specify multiple `[ExcludedFromScanScope.item_#]` sections.

   The application processes the scopes by index in ascending order.

   e. Save the changes in the configuration file.

   f. Import settings from the configuration file to the task using the following command:

   ```
   kesl-control --set-settings <task ID|name> --file <path>
   ```

3. If necessary, you can delete an exclusion scope by running the following command:

   ```
   kesl-control --set-settings <task ID|name> --del-exclusion <path>
   ```

   where:

   - `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
   - `--del-exclusion <path>` removes a path to a directory with objects to be excluded from scanning.

   The `[ExcludedFromScanScope.item_#]` section that contains the specified path will be deleted from the task settings. The application will not exclude the objects in the specified directory from the scan.

How to optimize Container Scan

Configure file scanning to optimize the performance of the task. This helps reduce CPU utilization on the protected device. You can limit the scanning of archives, set the maximum size of objects that can be scanned, and set the maximum object scan duration. Kaspersky Endpoint Security also allows excluding from scanning files of certain formats: archives, email databases, text files, and plain text email messages.

How to configure file scanning in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. In the list of tasks, select the Kaspersky Endpoint Security Container Scan task and click the name of the task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Under **Scan settings**, configure file scanning:

   - **Scan archives**. This includes the scanning of ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE and other types of archives. The application identifies archives not just by extension, but also by format. When scanning archives, the application performs recursive unpacking. This makes it possible to detect threats in nested archives (archive inside an archive). The scan is disabled by default.

   - **Scan SFX archives**. Scan of self-extracting archives that contain an executable extraction module. The scan is disabled by default.

   - **Scan mail databases**. Scanning email databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail clients. The scan is disabled by default.

   - **Scan mail format files**. Scan plain text email messages. The scan is disabled by default.

   - **Skip file that is scanned for longer than (sec)**. Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting. By default, the application tries to scan an object within one minute.

   - **Skip file larger than (MB)**. Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.

   - **Skip file larger than (MB)**. Postponed start of scan tasks if a scan is already running. Kaspersky Endpoint Security will enqueue new scan tasks if the current scan continues. This helps optimize the load on the computer. For example, let's assume that the application has started a Full Scan task according to the schedule. If a user attempts to start a quick scan from the application interface, Kaspersky Endpoint Security will enqueue this quick scan task and then automatically start this task after the Full Scan task is finished.

5. Save your changes.

How to configure file scanning on the command line

1. Run the following command:

```
kesl --set-settings <task ID|name> ScanArchived=<Yes|No> ScanSfxArchived=<Yes|No> ScanMailBases=<Yes|No>
ScanPlainMail=<Yes|No> SkipPlainTextFiles=<Yes|No> SkipDatabaseJournals=<Yes|No> SizeLimit=<object size (MB)>
TimeLimit=<scan time (sec)> QueueScanTasks=<Yes|No>
```

   where:

   - `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
   - `<object size (MB)>` is the maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object. Default value: `0`.
   - `<scan time (sec)>` is the maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting. Default value: `0`.

2. You can also configure the settings using a configuration file:

   a. Output task settings to a configuration file by running the following command:

```
kesl-control --get-settings <task ID|name> [--json]
```

   b. Open the configuration file for editing.

   c. To this file, add the following *Container Scan* task settings that apply to objects inside containers and images: `ScanArchived`, `ScanSfxArchived`, `ScanMailBases`, `ScanPlainMail`, `SizeLimit`, `TimeLimit`, `QueueScanTasks`.

   d. Save the changes in the configuration file.

   e. Import settings from the configuration file to the task using the following command:

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

   where:

   - `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
   - `--file <path>` is the full path to the configuration file from which you want to import the task settings.
   - Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

   All values of the task settings defined in the file will be imported into the application.

How to select an action to be performed on a container when an infected object is detected

When an infected object is detected in a container, Kaspersky Endpoint Security can immediately stop the container, take no action, or stop the container disinfecting the object or eliminating the threat has proved impossible. You can select the action that Kaspersky Endpoint Security performs with the container when an infected object is detected as part of real-time scanning by the *Container Monitoring* component or as part of an on-demand *Container Scan* task.

If an infected object is detected in the container image, Kaspersky Endpoint Security may delete the image or take no action with the image. You can select the action that Kaspersky Endpoint Security performs with the container image when an infected object is detected as part of an on-demand *Container Scan* task.

How to select a Container Monitoring action on threat detection in the Web Console

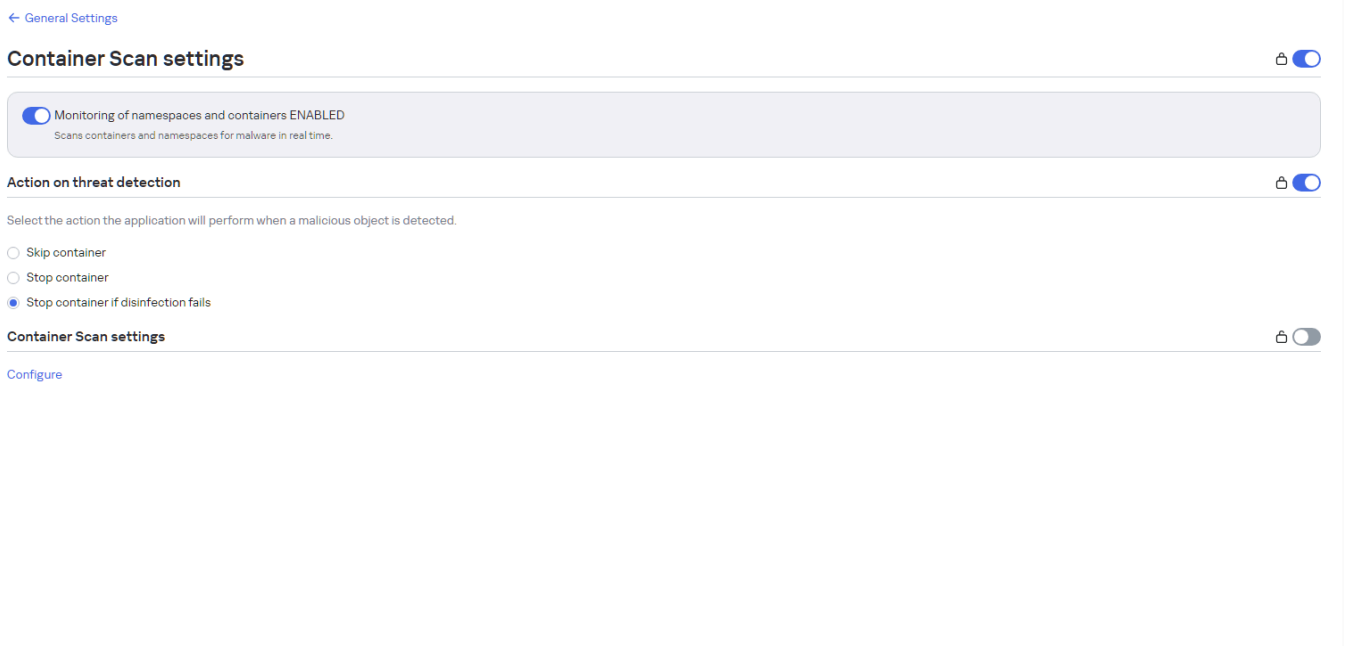
1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Container Scan settings**.
5. Make sure the toggle switch for the Container Monitoring component is in the **Monitoring of namespaces and containers ENABLED** position.
6. Under **Action on threat detection**, select the action that the application will take when an infected object is detected in a container:

   - **Skip container**. When an infected object is detected in a container, the application does not perform any actions with the container.
   - **Stop container**. When an infected object is detected in a container, the application stops the container.
   - **Stop container if disinfection fails** (default). When an infected object is detected in a container, the application attempts to disinfect the infected object. If an infected object could not be disinfected, the application stops the container.

     > Due to the way a CRI-O environment works, an infected object is not disinfected or deleted in a container in a CRI-O environment. We recommend selecting the **Stop container** action.

7. Save your changes.



Container Scan settings

How to select a Container Monitoring action on threat detection on the command line

1. Run the following command:

```
kesl-control --set-container-settings OnAccessContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
```

> This setting can only be configured when using the application under a license that supports this function.

2. To check the current values of the Container Scan settings, run the following command:

```
kesl-control --get-settings container-settings
```

How to select a Container Scan action on threat detection in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. In the list of tasks, select the Kaspersky Endpoint Security Container Scan task and click the name of the task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Under **Advanced scan settings** → **Container Scan settings** → **Action on threat detection**, select the action that the application will take when an infected object is detected in a container:

   - **Skip container**. When an infected object is detected in a container, the application does not perform any actions with the container.

   - **Stop container**. When an infected object is detected in a container, the application stops the container.

- **Stop container if disinfection fails** (default). When an infected object is detected in a container, the application attempts to disinfect the infected object. If an infected object could not be disinfected, the application stops the container.

> Due to the way a CRI-O environment works, an infected object is not disinfected or deleted in a container in a CRI-O environment. We recommend selecting the **Stop container** action.

5. Under **Advanced scan settings** → **Image scan settings** → **Action on threat detection**, select the action that the application will take when an infected object is detected in a container:

   - **Skip image** (default). When an infected object is detected in the image, the application does not perform any actions on the image.

   - **Delete image** (not recommended). When an infected object is detected in the image, the application deletes the image. All dependencies will also be deleted. Running containers will be stopped, and then deleted.

6. Save your changes.

How to select a Container Scan action on threat detection on the command line

1. Run the following command:

```
kesl-control --set-settings <task ID|name> ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>
ImageAction=<Skip|Delete>
```

   Where `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

> Due to the way a CRI-O environment works, an infected object is not disinfected or deleted in a container in a CRI-O environment. We recommend selecting the `StopContainer` action.

2. You can also configure the action using a configuration file:

   a. Output task settings to a configuration file by running the following command:

```
kesl-control --get-settings <task ID|name> [--json]
```

   b. Open the configuration file for editing.

   c. Add the following settings of the *Container Scan* task to the file:

   - `ContainerScanAction=<Skip|StopContainer|StopContainerIfFailed>` – action to be performed on a container when an infected object is detected. Default value: `StopContainerIfFailed`.

   - `ImageAction=<Skip|Delete>` – action to be performed on a container image when an infected object is detected. Default value: `Skip`.

   d. Save the changes in the configuration file.

e. Import settings from the configuration file to the task using the following command:

```
kesl-control --set-settings <task ID|name> --file <path> [--json]
```

Where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `--file <path>` is the full path to the configuration file from which you want to import the task settings.
- Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

All values of the task settings defined in the file will be imported into the application.

How to run a custom scan of containers and images

To start the Custom Container Scan task on the command line, run the following command:

```
kesl-control --scan-container <id|name[:tag]>
```

where `<id|name[:tag]>` is the name or ID of the container or image. You can use masks to scan multiple objects.

If there are several entities with the same name, the application scans all of them.

As a result of executing the command, a temporary containers and images scan task is created, which is automatically deleted after completion. In this case, the scan results are output to the console.

```
Example of a container scan performed on a container named my_container
kesl-control --scan-container my_container
```

```
Example of an image scan performed on an image named my_image (all tags)
kesl-control --scan-container my_image*
```

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Removable drives scan

Kaspersky Endpoint Security scans all files that you execute or copy, even if the file is located on a removable drive. The application scans files on CDs, DVDs, Blu-ray discs, flash drives (including USB modems), external hard drives, and floppy disks. By default, Removable Drives Scan is disabled.

How Removable Drives Scan works

When a removable drive is connected, the application automatically creates and starts the following scan tasks with default settings: *Critical Areas Scan* for the quick scan and *Malware Scan* for the detailed scan. These tasks cannot be stopped. When a threat is detected on the removable drive, Kaspersky Endpoint Security tries to disinfect the infected object. If disinfection proves impossible, the application deletes the infected object. After the scan is completed, the application deletes these tasks automatically.

Scan types

- **Quick Scan**. Kaspersky Endpoint Security scans only files with specified extensions and does not unpack compound objects. The application performs a quick scan with the default settings of *Critical Areas Scan* the task.
- **Detailed Scan**. Kaspersky Endpoint Security scans all files on removable drives. The application performs a detailed scan with the default settings of the *Malware Scan* task.

How to select a Removable Drives Scan type in the Web Console

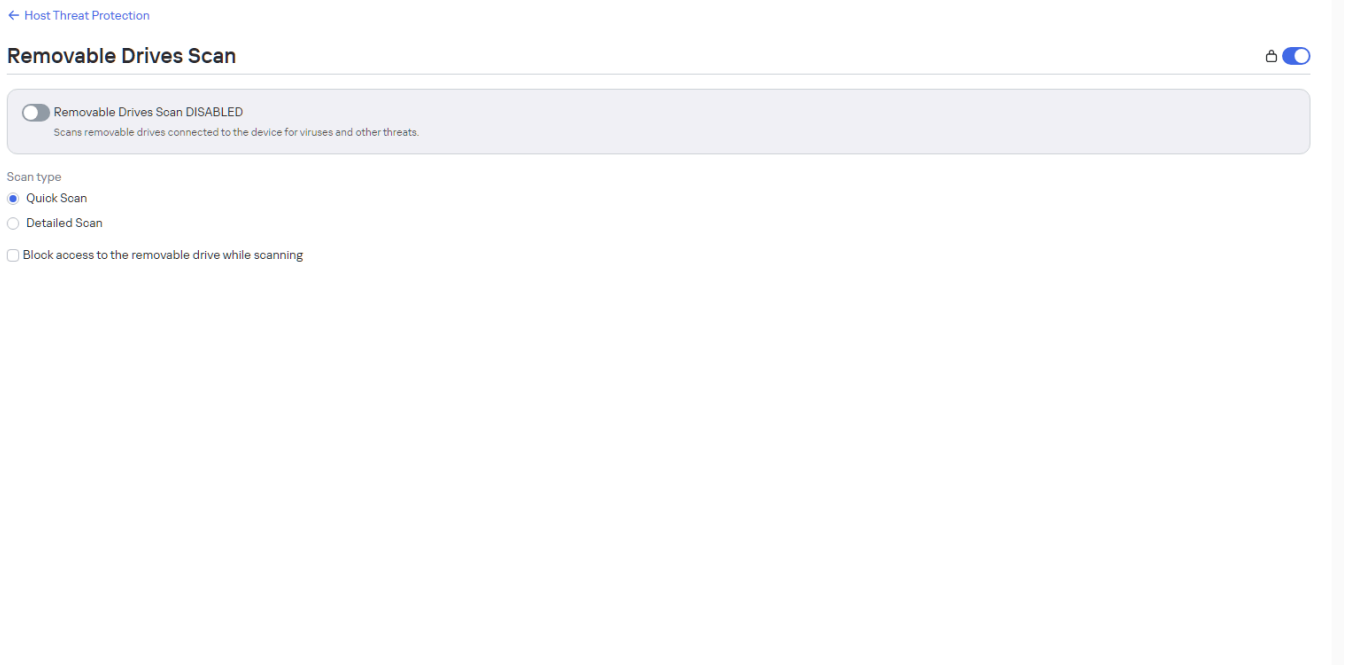
1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **Removable Drives Scan**.
5. Make sure the toggle switch for the component is in the **Removable Drives Scan ENABLED** position.
6. Under **Scan type**, select the type of Removable Drives Scan: **Quick Scan** or **Detailed Scan**.
7. If necessary, select the **Block access to files during scans** check box.

   Blocking access to files prevents a user from running malware while the scan is in progress.

While scanning boot sectors, the application does not block any files.

8. To apply the policy to computers, close the padlock icons and save your changes.



Removable drives scan

How to select a Removable Drives Scan type on the command line

1. Select the type of scan to perform when connecting removable drives:

```
kesl-control --set-settings 16 ScanRemovableDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

2. Select the type of scan to perform when CD/DVD drives or Blu-ray discs are inserted:

```
kesl-control --set-settings 16 ScanOpticalDrives=<DetailedScan|QuickScan|NoScan> BlockDuringScan=<Yes|No>
```

3. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 16
```

Symbols

Command options

Setting	Description
`ScanRemovableDrives`	Type of scan when removable drives are connected: • `DetailedScan`. Detailed Scan. • `QuickScan`. Quick Scan. • `NoScan` (default). The application does not perform a scan.
`ScanOpticalDrives`	Type of scan to perform when CD/DVD drives or Blu-ray discs are inserted: • `DetailedScan`. Detailed Scan. • `QuickScan`. Quick Scan. • `NoScan` (default). The application does not perform a scan.

Setting	Description
`BlockDuringScan`	Block access to files on the connected disk during scanning. By default, the application does not block access to files. Blocking access to files prevents a user from running malware while the scan is in progress. While scanning boot sectors, the application does not block any files.

Behavior Detection

The Behavior Detection component allows monitoring the activity (opening files, establishing connections, etc.) of applications that can compromise the computer or user data. The component monitors application behavior looking for dangerous patterns. If application activity matches one of such patterns, Kaspersky Endpoint Security performs the selected responsive action. This functionality of Kaspersky Endpoint Security provides proactive protection of the computer.

For optimal performance of the Behavior Detection component, we recommend enabling the Web Threat Protection component.

How Behavior Detection works

1. **The application monitors events in the operating system**

   The application receives a stream of telemetry consisting of events: process creation and termination, opened files, established connections, etc. The application also enriches events with relevant metadata (process name, PID, IP address, and so on).

2. **The application compares the telemetry stream with patterns of dangerous behavior**

   If the actions of a third-party application match a dangerous behavior pattern, Kaspersky Endpoint Security performs a threat response action (for example, it can stop the third-party application).

3. **The application sends telemetry to KSN**

   The application filters events and sends them to KSN for further analysis.

Configuring Behavior Detection

1. **In the Behavior Detection settings, select the Inform action**

   By default, the Behavior Detection component is enabled. In the Behavior Detection settings, we recommend selecting **Inform** as the action on threat detection and checking if the installed applications can work normally. Kaspersky Endpoint Security allows all application activity and keeps a log of the component's operation.

   How to select an action on malware activity detection in the Web Console

   1. In the main window of the Web Console, select **Asset management** → **Policies**.
   2. Click the name of the Kaspersky Endpoint Security policy.

      The policy properties window opens.

3. Select the **Application settings** tab.

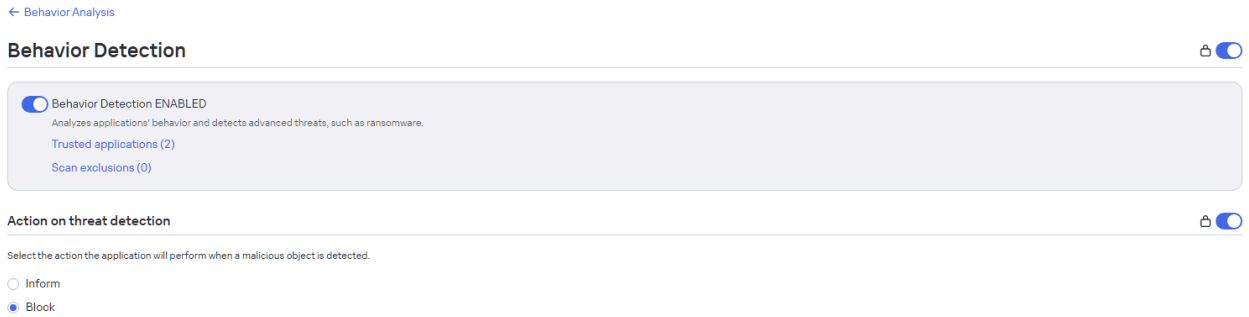
4. Go to **Host Threat Protection** → **Behavior Analysis** → **Behavior Detection**.

5. Select the relevant action in the **Action on threat detection** block:

   - **Inform**. If malicious activity is detected, Kaspersky Endpoint Security does not stop this application, but only logs an event about the detection of malicious activity in the event log.

   - **Block**. If malicious activity is detected, Kaspersky Endpoint Security stops the process of the application that is carrying out the malicious activity and logs information about the detected malicious activity.

6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Behavior Detection

How to select an action on malware activity detection on the command line

1. Run the following command:

```
kesl-control --set-settings 20 TaskMode=<Block|Notify>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 20
```

Symbols

Command options

Setting	Description
`TaskMode`	Action on malware activity detection: • `Block` (default). If malicious activity is detected, Kaspersky Endpoint Security stops the process of the application that is carrying out the malicious activity and logs information about the detected malicious activity. • `Notify`. If malicious activity is detected, Kaspersky Endpoint Security does not stop this application, but only logs an event about the detection of malicious activity in the event log.

2 Collect Behavior Detection statistics

You can get Behavior Detection statistics using reports.

3. **Optimize application performance**

   After analyzing the gathered information, optimize application performance and add exclusions.

4. **In the Behavior Detection settings, select the Block action**

   Turn on blocking of malicious activity of applications. After that, Kaspersky Endpoint Security will stop the processes of applications that are carrying out malicious activity.

Special considerations and limitations

- For correct operation of the Behavior Detection component when Kaspersky Endpoint Security is integrated with Kaspersky Managed Detection and Response and Kaspersky Anti Targeted Attack Platform solutions, make sure that auditd is set to no configuration blocking mode `enabled 1` in the configuration files.

Exploit Prevention

Exploit Prevention monitors code that exploits vulnerabilities on your device to gain administrative privileges or perform malicious actions.

For the Exploit Prevention component to work, the following components must be enabled:

- Behavior Detection
- Updatable kernel module

> The component is not available for devices with an Elbrus CPU.

How Exploit Prevention works

1. **The application monitors events in the operating system**

   The application receives a stream of telemetry consisting of events: process creation and termination, opened files, established connections, etc. The application also enriches events with relevant metadata (process name, PID, IP address, and so on).

2. **The application compares the telemetry stream with patterns of dangerous behavior**

   If the actions of a third-party application match a dangerous behavior pattern, Kaspersky Endpoint Security performs a threat response action (for example, it can stop the third-party application).

Configuring Exploit Prevention

1. **In the Exploit Prevention settings, select the Inform action**

By default, the Exploit Prevention component is disabled. In the Exploit Prevention settings, select **Inform** as the action on threat detection and check if the installed applications can work normally. Kaspersky Endpoint Security allows all application activity and logs information about detected threats.

How to select the action on exploit detection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **Behavior Analysis** → **Exploit Prevention**.
5. Use the **Exploit Prevention** toggle to enable or disable the component.
6. Select the relevant action in the **Action on threat detection** block:
   - **Block**. If this item is selected, on detecting an exploit, Kaspersky Endpoint Security blocks the operations of this exploit and makes a log entry with information about this exploit.
   - **Inform**. If this item is selected, when Kaspersky Endpoint Security detects an exploit, it logs an entry containing information about the exploit and adds information about this exploit to the list of active threats.
7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to select the action on threat detection on the command line

1. To enable Exploit Prevention, run the following command:

```
kesl-control --set-settings 20 UseAEP=Yes
```

2. Select an action on exploit detection:

```
kesl-control --set-settings 20 AEPMode=<Block|Notify>
```

3. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 20
```

Symbols

Command options

Setting	Description
`UseAEP`	Enabling the component: • `Yes` enables Exploit Prevention. • `No` (default) disables Exploit Prevention.

Setting	Description
AEPMode	Action on exploit detection: • `Block` (default). Kaspersky Endpoint Security blocks the operations of this exploit and makes a log record with information about this exploit. • `Notify`. Kaspersky Endpoint Security detects an exploit, it makes a log record with information about the exploit and adds information about this exploit to the list of active threats.

2. **Collect Exploit Prevention statistics**

   You can get Exploit Prevention statistics using reports.

3. **Optimize application performance**

   After analyzing the gathered information, optimize application performance:

   - Add global exclusions
   - Add exclusions

4. **In the Exploit Prevention settings, select the Block action**

   Enable the blocking of malicious activity of applications in the operating system.

Anti-Cryptor

The Anti-Cryptor component provides protection against remote encryption by analyzing the activity of remote devices in shared network directories of the computer. Anti-Cryptor analyzes files that are transmitted to the protected computer via the NFS and SMB protocols.

If activity matches a behavior stream signature that is typical for external encryption, Kaspersky Endpoint Security blocks this activity or informs you about it.

How Anti-Cryptor works

1. **The application intercepts NFS and SMB requests**

   The application receives a stream of telemetry about the creation and modification of files transmitted via the NFS and SMB protocols.

2. **The application compares the telemetry stream with databases of signatures.**

   If the actions of the third-party application match those of ransomware, Kaspersky Endpoint Security performs the selected action on threat detection (for example, blocking the connection to the remote computer).

Configuring Anti-Cryptor

1. **Configure the protection scope**

   By default, the application scans all shared directories. If you only need to scan an individual directory (for example, the directory into which files are automatically downloaded from an external source), you can specify only that directory as the protection scope. In other cases, we recommend keeping the default protection scope and using exclusions to fine-tune the scope.

2. **In the Anti-Cryptor settings, select the Inform action**

   By default, Anti-Cryptor is disabled. We recommend enabling Anti-Cryptor, and as the action on threat detection, selecting **Inform** and checking access to all corporate resources. Kaspersky Endpoint Security allows access to all resources in shared directories and logs information about detected threats.

3. **Collect Anti-Cryptor statistics**

   You can get Anti-Cryptor statistics using reports.

4. **Optimize application performance**

   After analyzing the gathered information, optimize application performance:

   - Add global exclusions.
   - Add exclusions.

5. **In the Anti-Cryptor settings, select the Block connection action**

   Enable the blocking of network traffic from a remote attacking device.

Special considerations and limitations

- The Anti-Cryptor component runs correctly with SMB1, SMB2, SMB3, NFS3, TCP/UDP, and IP protocols. Working with NFS2 and NFS4 protocols is not supported. It is recommended to configure your server so that the NFS2 and NFS4 protocols cannot be used to mount resources.
- For the Anti-Cryptor component to operate correctly, at least one of the services (Samba or NFS) must be installed in the operating system. For the NFS service, the rpcbind package must be installed.
- Kaspersky Endpoint Security does not block access to network file resources until the activity of a remote device is identified as malicious. So, at least one file will be encrypted before the application detects malicious activity.

How to select an action on malicious encryption detection

If malicious encryption is detected, the application can block network traffic for a remote attacking device or just inform about the detection of malicious encryption.

To block network traffic, Kaspersky Endpoint Security creates a dynamic firewall rule. The firewall temporarily blocks network traffic for the attacking device. The application also adds the attacking device to the list of blocked devices. Access to shared network directories is denied to blocked devices.

To inform the administrator about the detection of malicious encryption, the application generates an *Encryption detected* event.

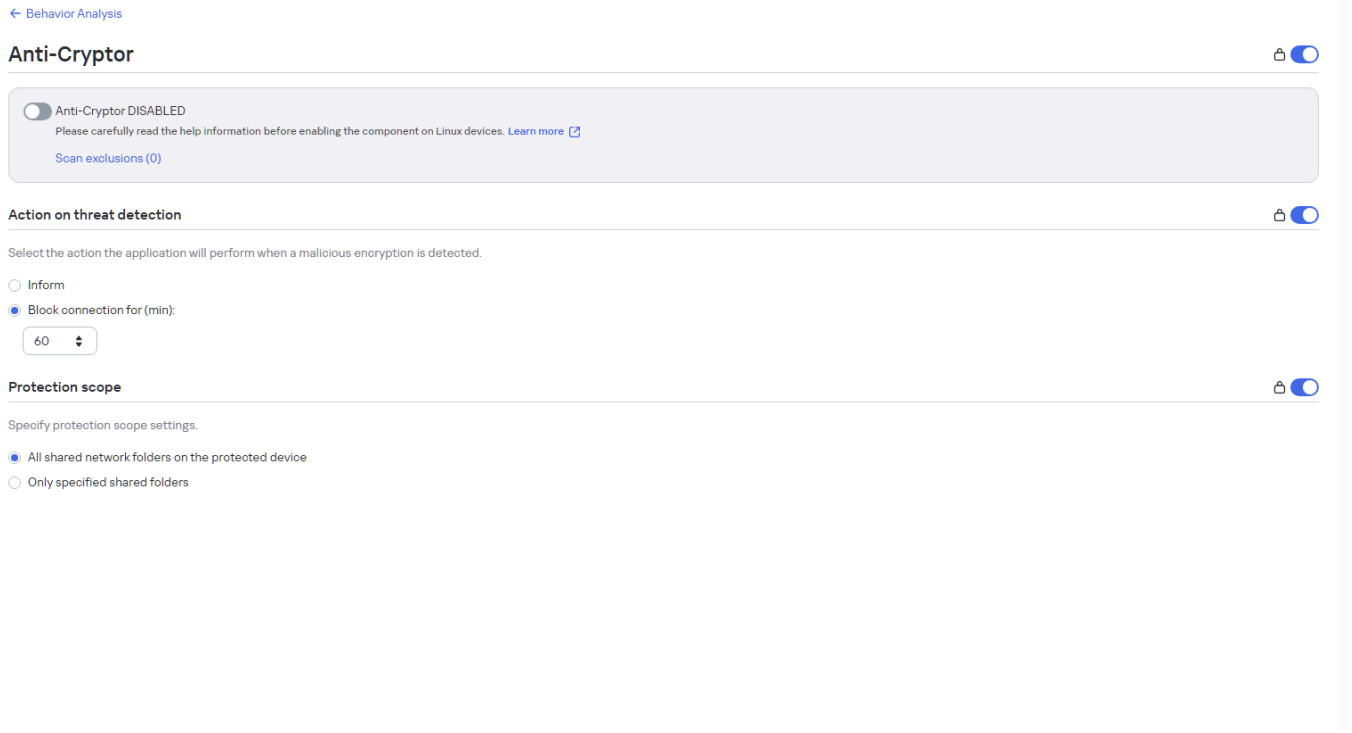
By default, the application blocks network traffic for an attacking device for 60 minutes. When the blocking time expires, the application removes the compromised device from the list of blocked devices, and the device's access to network file resources is automatically restored.

You can view the list of blocked devices and manually unblock these devices locally on the user's computer. Kaspersky Security Center does not provide tools for monitoring and managing blocked devices, other than the *Encryption detected* event.

How to configure actions on malicious encryption detection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Make sure the toggle switch for the component is in the **Anti-Cryptor ENABLED** position.
6. Under **Action on threat detection**, select the action that the application will take when a threat is detected: **Inform** or **Block connection for (min)**.
7. If **Block connection for (min)** is selected, set the blocking period of the attacking device in minutes. By default, the device is blocked for 60 minutes.
8. To apply the policy to computers, close the padlock icons and save your changes.



Anti-Cryptor

How to configure actions on malicious encryption detection on the command line

1. Run the following command:

```
kesl-control --set-settings 13 ActionOnDetect=<Block|Notify>
```

2. Select the blocking period for the `Block` action.

```
kesl-control --set-settings 13 BlockTime=<Blocking period>
```

3. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 13
```

Symbols

Command options

Setting	Description
`ActionOnDetect`	Action on external encryption detection: • `Block` (default) blocks network traffic for the attacking device and creates an *Encryption detected* event. • `Notify` creates an *Encryption detected* event without blocking network traffic.
`BlockTime`	Blocking period of the attacking devices in minutes.

How to create a protection scope

A *protection scope* is a list of paths to shared network directories in which Kaspersky Endpoint Security monitors file activity. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask. By default, the application automatically identifies shared network directories and monitors file activity in these directories.

If necessary, you can restrict file activity monitoring for malicious encryption to a subset of directories. Kaspersky Endpoint Security scans objects in the specified scopes in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

Excluding a directory from the protection scope can reduce the amount of false positives if your organization uses data encryption when exchanging files via shared network directories. For example, Anti-Cryptor can raise false positives when the user works with files with the ENC extension in a shared folder. Such activity matches a behavioral pattern that is typical for external encryption. If you have encrypted files in a shared network directory to protect data, add that directory to exclusions.

How to create a protection scope in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **Behavior Analysis** → **Anti-Cryptor**.
5. Make sure the toggle switch for the component is in the **Anti-Cryptor ENABLED** position.
6. Under **Protection scope**, select **Only specified shared folders**.
7. In the list of directories, click **Add**.

8. This opens a window; in that window, select the type of file system:
   - **Local**. Directories on the hard drive accessible without a network connection.
   - **Shared**. Computer directories accessible via the Samba (SMB) or NFS protocol.
   - **All shared**. All computer directories accessed via the Samba and NFS protocols.
9. For a local file system, specify a directory path (for example, `/path/to/folder`).
10. Specify masks for object extensions (for example, `*.txt`). Separate masks with commas.
11. To apply the policy to computers, close the padlock icons and save your changes.

How to create a protection scope on the command line

1. Run the following command:

```
kesl-control --set-settings 13 ScanScope.item_#.UseScanArea=Yes \
        [ScanScope.item_#.AreaDesc=<description of the area>] \
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>] \
        [ScanScope.item_#.Path=<path to the directory>]
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 13
```

Symbols

Command options

Setting	Description
`ScanScope.item_#.UseScanArea=Yes`	Enabling a protection scope number `#`. You can temporarily exclude a protection scope instead of deleting it. To do this, set `ScanScope.item_#.UseScanArea=No`.
`ScanScope.item_#.AreaDesc`	Description of protection scope; contains additional information about the `#` protection scope.

`ScanScope.item_#.AreaMask.item_#`	Protection scope limitation. In the protection scope, the application protects only the objects that are specified using the masks in the shell format.
	`Example`
	`ScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt.`

`ScanScope.item_#.Path`	Path to the directory with the objects to be protected. Possible values: • `AllShared` (default). All computer directories accessed via the Samba and NFS protocols. • `Shared:SMB`. Directories accessible via the Samba (SMB) protocol. • `Shared:NFS`. Directories accessible via the NFS protocol. • `<path to local directory>`. Directories on the hard drive accessible without a network connection. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

Example of a protection scope that includes only the /home directory

```
kesl-control --set-settings 13 ScanScope.item_0001.UseScanArea=Yes ScanScope.item_0001.Path=/home
```

BadUSB Attack Prevention

Attackers can exploit vulnerabilities in the firmware of a USB device (for example, a flash drive) and reprogram the device to make the operating system recognize this device as a keyboard when connected. As a result, an infected USB device may execute commands under your user account to, for example, download malware.

The BadUSB Attack Prevention protection component allows preventing the connection of an infected USB device.

The component is not available for devices with an Elbrus CPU.

How BadUSB Attack Prevention works

1. **The application prompts you to authorize the USB device**

   When a USB device is connected to the device, the application prompts the user to enter a numerical code generated by the application. This procedure is known as *authorization*.

2. **The user enters the authorization code**

   The user can enter the code using the connected USB device itself (keyboard or barcode scanner) or an on-screen keyboard, if available. You cannot enter the code using a USB device that is already connected.

3. **The application allows authorized USB devices and blocks unauthorized USB devices**

   If the numeric code is entered correctly, the application saves the identification parameters, that is, the VID/PID of the USB device and the port number to which it is connected, in the list of authorized USB devices. This USB device will not need to be authorized again if it is reconnected or if the operating system is restarted.

   If the numeric code is entered incorrectly, the application generates a new code. You can configure the maximum number of attempts for entering the numerical code. If the numeric code is entered incorrectly several times, the application blocks input from this USB device for a certain time. After waiting for the USB device lockout time to elapse, you can make more attempts to authorize the USB device. You can configure the time after which you can continue to try entering the authorization code.

When an authorized USB device is connected to a different USB port, the application requires it to be authorized again.

Configuring BadUSB Attack Prevention

1. **Enable BadUSB Attack Prevention**

   By default, the BadUSB Attack Prevention protection component is disabled. Identify devices to which untrusted individuals can gain physical access to and that need to be protected from outside attackers, and enable the BadUSB Attack Protection component on these devices. After enabling BadUSB Attack Protection, the application will require authorization of connected USB devices, and users will not be able to use unauthorized USB devices until they are authorized. However, USB devices connected before BadUSB Attack Protection was enabled are considered authorized by default and do not require authorization.

   > Do not connect any untrusted USB devices to the device until you enable and configure BadUSB Attack Protection.

2. **Configure BadUSB Attack Prevention**

   Depending on the type of USB devices being connected (keyboards or barcode scanners), configure how you want the authorization code to be displayed: as a barcode or as a numeric code (default setting).

   If necessary, configure USB device authorization:

   - The maximum number of attempts to enter the authorization code
   - USB device blocking duration when the maximum number of attempts is reached.

How to configure USB device authorization

When a USB device that the operating system identifies as an input device is connected to the managed device, the application suggests authorizing the USB device using a numeric code or barcode. If the authorization code has been entered incorrectly, the application generates a new code. If the authorization code is entered incorrectly multiple times or the authorization window is closed, the application blocks input from this USB device. When the USB device blocking time elapses or the operating system is restarted, the application prompts the user to perform authorization again.

Kaspersky Endpoint Security allows you to configure USB device authorization

- Maximum number of authorization attempts.
- USB device blocking duration when the maximum number of attempts is reached.

How to configure USB device authorization in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

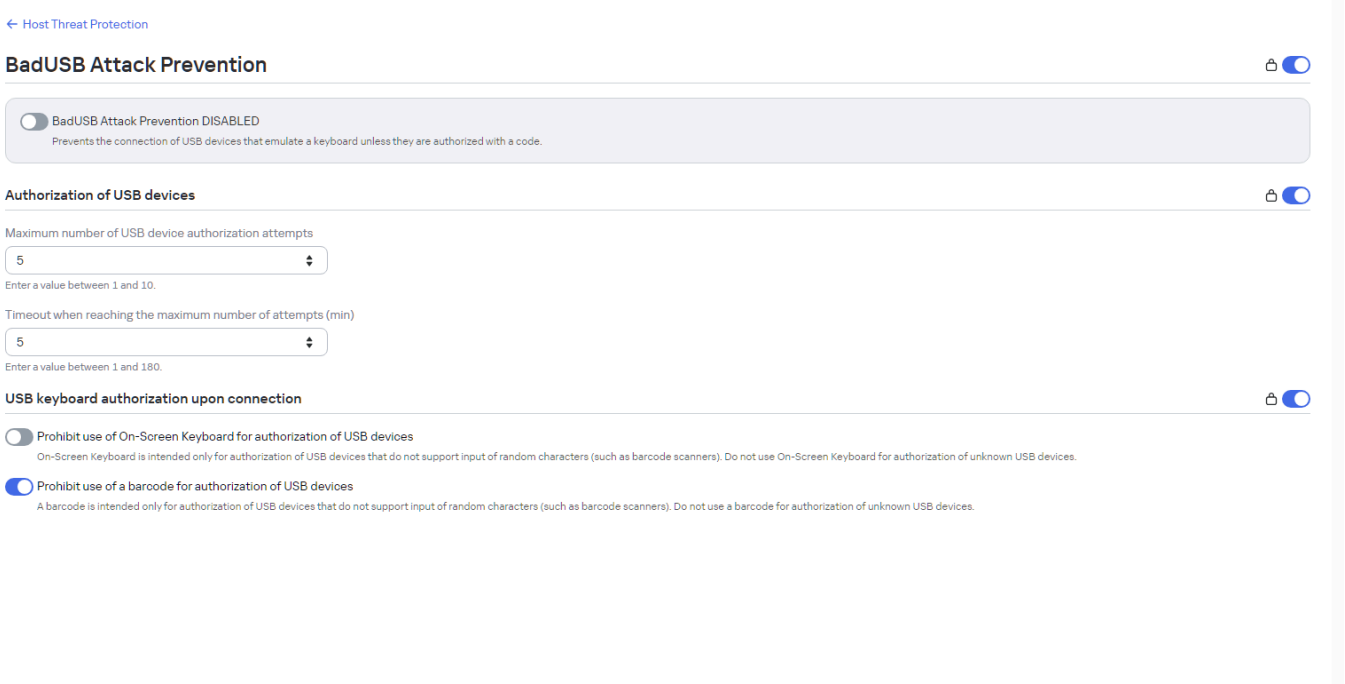
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Make sure the toggle switch for the component is in the **BadUSB Attack Prevention ENABLED** position.

6. Under **Authorization of USB devices**, configure authorization settings:

- **Maximum number of USB device authorization attempts**. Automatically block the USB device if the authorization code is entered incorrectly the specified number of times. Valid values are 1 to 10. For example, if you allow five attempts to enter the authorization code, the application blocks the USB device after the fifth unsuccessful attempt. Kaspersky Endpoint Security displays the time for which the USB device is blocked. After this time elapses, you will once again have five attempts to enter the authorization code.

- **Timeout when reaching the maximum number of attempts (min)**. USB device block duration after the specified number of unsuccessful attempts to enter the authorization code. Possible values: 1 to 180 (minutes)

7. To apply the policy to computers, close the padlock icons and save your changes.



BadUSB Attack Prevention

How to configure USB device authorization on the command line

1. Run the following command:

```
kesl-control --set-settings 37 MaxAuthAttempts=<number of attempts> TimeoutAfterAttempts=<timeout (minutes)>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 37
```

Symbols

Command options

Setting	Description
`MaxAuthAttempts`	Automatically block the USB device if the authorization code is entered incorrectly the specified number of times. Valid values are 1 to 10. For example, if you allow five attempts to enter the authorization code, the application blocks the USB device after the fifth unsuccessful attempt. Kaspersky Endpoint Security displays the time for which the USB device is blocked. After this time elapses, you will once again have five attempts to enter the authorization code. Default value: 5.
`TimeoutAfterAttempts`	USB device block duration after the specified number of unsuccessful attempts to enter the authorization code. Possible values: 1 to 180 (minutes) Default value: 5 minutes.

How to allow connecting USB devices using the on-screen keyboard

On-Screen Keyboard should be used only for authorization of USB devices that do not support the input of random characters (such as barcode scanners). It is not recommended to use On-Screen Keyboard for authorization of unknown USB devices. By default, using the on-screen keyboard is allowed.

We recommend using the on-screen keyboard only for authorizing USB devices known to the user.

How to enable USB device authorization using the on-screen keyboard in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Make sure the toggle switch for the component is in the **BadUSB Attack Prevention ENABLED** position.
6. Make sure the **Prohibit use of On-Screen Keyboard for authorization of USB devices** toggle switch is off. The toggle button is switched off by default.
7. To apply the policy to devices, close the 🔒 padlock icons and save your changes.

How to enable USB device authorization using the on-screen keyboard on the command line

Execute the command:

```
kesl-control --set-settings 37 ProhibitOnScreenKeyboard=No
```

How to allow connecting USB devices using the barcode scanner

When connecting a barcode scanner to the device, the BadUSB Attack Prevention component identifies this scanner as an input device and prompts you to perform authorization. To authorize the barcode scanner, you must scan a barcode displayed on the screen. The application generates a barcode in the Code39 format. Most barcode scanners and QR code scanners support this format.

The application also supports another way of authorizing barcode scanners. If you are using touchscreen devices, you can use an on-screen keyboard to type a code. To do so, you need to allow the on-screen keyboard. This method is convenient, for example, in the case of stationary barcode scanners built into cash registers. Other barcode scanner authorization methods are forbidden. By default the application does not use a barcode for authorization of USB devices.

How to enable USB device authorization using the barcode scanner in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Host Threat Protection** → **BadUSB Attack Prevention**.
5. Make sure the toggle switch for the component is in the **BadUSB Attack Prevention ENABLED** position.
6. Disable the **Prohibit use of a barcode for authorization of USB devices** toggle switch.
7. To apply the policy to devices, close the 🔒 padlock icons and save your changes.

How to enable USB device authorization using the barcode scanner on the command line

Execute the command:

```
kesl-control --set-settings 37 ProhibitBarcodeScanner=No
```

Communication & Web Protection

Mail Threat Protection

The Mail Threat Protection component scans the attachments of incoming and outgoing email messages for viruses and other threatening applications. This component protects the device using anti-virus databases, the Kaspersky Security Network cloud service, and heuristic analysis.

Mail Threat Protection can scan incoming as well as outgoing messages. The application supports POP3, SMTP, and IMAP in the following mail clients: The application also supports extended versions of protocols: POP3S, SMTPS, and IMAPS.

The Mail Threat Protection component does not scan messages if the mail client is open in a browser.

> For the Mail Threat Protection component to work, network ports 25, 110, 143, 465, 587, 993, and 995 must be monitored in the network settings. These network ports are added to the list of monitored ports by default. Removing these ports from the list may prevent the component from working correctly.

By default, the Mail Threat Protection component is enabled.

How Mail Threat Protection works

When installing Kaspersky Endpoint Security, the application adds a self-signed certificate, *Kaspersky Anti-Virus Personal Root Certificate*. The application places this certificate in the local trusted certificate store (`/etc/ssl/certs`). Every time the application starts, it checks if the certificate is present. If the certificate has been deleted, the application restores the certificate automatically.

1. **The application intercepts mail traffic**

   Kaspersky Endpoint Security checks the connection via POP3, SMTP, and IMAP protocols.

2. **The application scans incoming as well as outgoing messages**

   Mail Threat Protection scans traffic using the following technologies:

   - Anti-virus databases.
   - Cloud services of Kaspersky Security Network.
   - The Heuristic analysis technology allows detecting threats that are not yet covered by Kaspersky databases.

3. **The application completes the scan**

   If an incoming message contains a threat in an attachment or in the body of the message, Kaspersky Endpoint Security performs an action on threat detection. If a threat is detected in an outgoing message, Mail Threat Protection blocks the sending of such a message.

Configuring Mail Threat Protection

1. **Define a group for test deployment of the component**

   Set apart a small group of devices on which you will test the configuration of the Mail Threat Protection component. This will let you make sure that the component is configured correctly and ensure the stable operation of the mail client, avoiding possible faults.

2. **Configure attachment filter**

   By default, the Mail Threat Protection filter as configured by Kaspersky provides the recommended level of protection. If you have special requirements for mail security, you can change the attachment filter settings.

3. **Configure message scanning**

   If necessary, configure email message scanning in accordance with the parameters of your mail server. For example, you can limit the size of the scanned archives to reduce the load on the mail server.

4. **Verify that Mail Threat Protection is working correctly**

   Generate a test message with a malicious attachment. Send the message to your selected group of devices and verify that the malicious content of the message has been processed in accordance with the component settings.

   You can also verify that the application has generated the corresponding *Threat detected* event by running the following command:

   ```
   kesl-control -E -q "TaskName == 'Mail_Monitoring'"
   ```

5. **Apply the Mail Threat Protection settings to all devices in the organization**

Special considerations and limitations

- If the mail client on the protected devices does not use a local store of trusted certificates, manually add the *Kaspersky Anti-Virus Personal Root Certificate* certificate to the trusted certificate store of the mail client. For more information on adding a certificate, see the official documentation of your mail client.
- Mail Threat Protection does not attempt to disinfect malicious attachments in outgoing mail. Outgoing messages with malicious attachments are either completely blocked or allowed through.

What to do if a mail threat is detected

When an infected object is detected in an attachment of an *outgoing message*, the application prevents it from being sent.

If an infected object is detected in an *incoming message* the application can attempt to disinfect the object and then either delete or block access to the object. Kaspersky Endpoint Security also adds information about the performed action to the message subject, for example, *[Message has been processed] <message subject>*.

When configuring Mail Threat Protection, you can select actions that Kaspersky Endpoint Security will perform when a threat is detected in email messages.

How to configure actions on threat detection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Communication & Web Protection** → **Mail Threat Protection**.

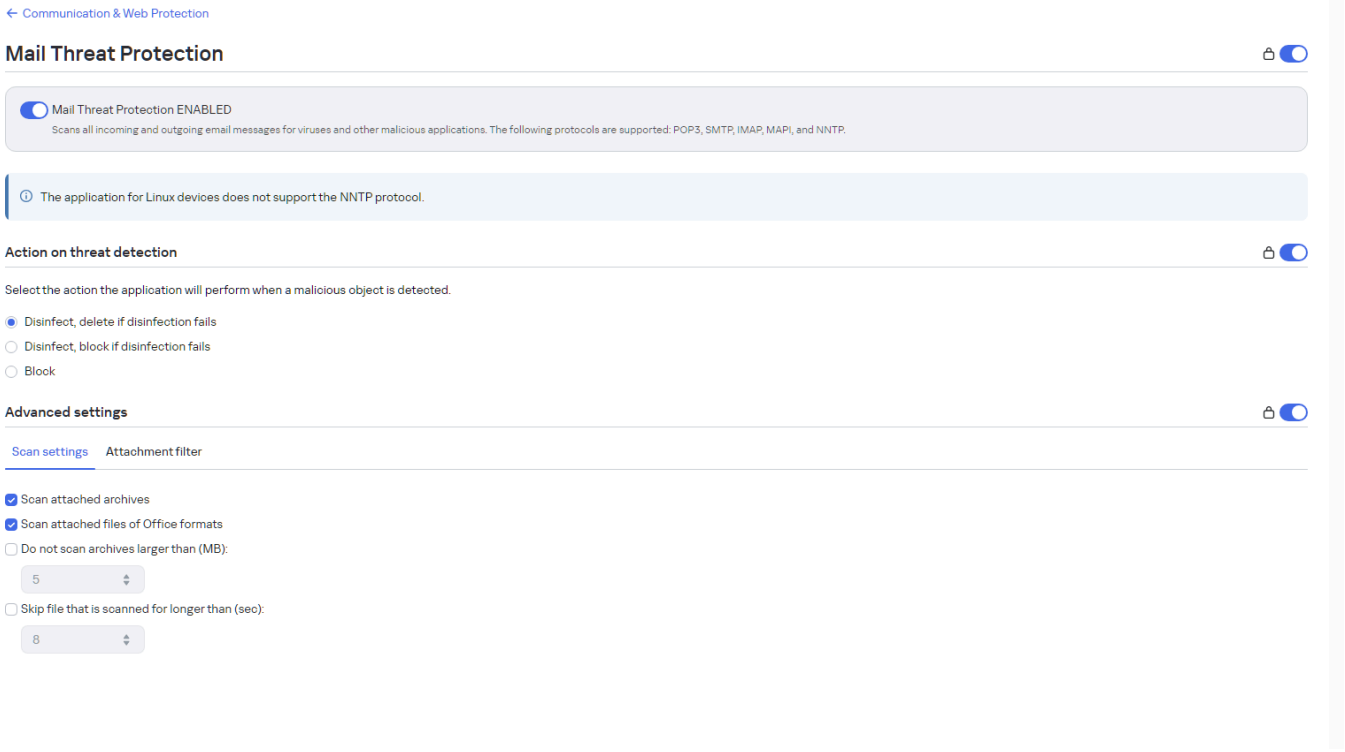
5. Under **Action on threat detection**, select the action that the application will take when a threat is detected:

   - **Disinfect, delete if disinfection fails**. When an infected object is detected in an incoming message, the application attempts to disinfect the detected object. The message with the safe attachment is then made available to the user. If disinfection fails, the application deletes the infected object. The application adds information about the performed action to the message subject, for example, *[The message has been processed] <message subject>*. If an infected object is detected in an outgoing message, the application blocks the message, and the mail client displays an error.

   - **Disinfect, block if disinfection fails**. When an infected object is detected in an incoming message, the application attempts to disinfect the detected object. The message with the safe attachment is then made available to the user. If disinfection fails, the application adds a warning to the subject of the message. The message with the original attachment is then made available to the user. If an infected object is detected in an outgoing message, the application blocks the message, and the mail client displays an error.

   - **Block**. If an infected object is detected in an incoming message, the application adds a warning to the message subject. The message with the original attachment is then made available to the user. If an infected object is detected in an outgoing message, the application blocks the message, and the mail client displays an error.

6. To apply the policy to computers, close the padlock icons and save your changes.



Mail Threat Protection

How to configure actions on threat detection on the command line

1. Make sure that the Mail Threat Protection component is enabled:

```
kesl-control --get-task-state 35
```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

```
kesl-control --start-task 35
```

3. Select an action to perform when a mail threat is detected in incoming messages:

```
kesl-control --set-settings 35 ActionOnThreat=<DisinfectDeleteIfNotPossible|DisinfectBlockIfNotPossible|Block>
```

4. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 35
```

Symbols

Command options

Setting	Description
`ActionOnThreat`	Action on threat detection: • `DisinfectDeleteIfNotPossible` (default). When an infected object is detected in an incoming message, the application attempts to disinfect the detected object. The message with the safe attachment is then made available to the user. If disinfection fails, the application deletes the infected object. The application adds information about the performed action to the message subject, for example, *[The message has been processed] <message subject>*. If an infected object is detected in an outgoing message, the application blocks the message, and the mail client displays an error. • `DisinfectBlockIfNotPossible`. When an infected object is detected in an incoming message, the application attempts to disinfect the detected object. The message with the safe attachment is then made available to the user. If disinfection fails, the application adds a warning to the subject of the message. The message with the original attachment is then made available to the user. If an infected object is detected in an outgoing message, the application blocks the message, and the mail client displays an error. • `Block`. If an infected object is detected in an incoming message, the application adds a warning to the message subject. The message with the original attachment is then made available to the user. If an infected object is detected in an outgoing message, the application blocks the message, and the mail client displays an error.

How to optimize email attachment scanning

Configure email attachment scanning to optimize the Mail Threat Protection component. This helps reduce CPU utilization on the protected device. You can limit the scanning of attached archives, set the maximum size of attachments that can be scanned, and set the maximum object scan duration.

How to optimize attachment scanning in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Communication & Web Protection** → **Mail Threat Protection**.

5. Under **Advanced settings**, select the **Scan settings** tab.

6. Configure attachment scanning:

- **Scan attached archives**. This includes the scanning of ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE and other types of archives. The application identifies archives not just by extension, but also by format. When scanning archives, the application performs recursive unpacking. This makes it possible to detect threats in nested archives (archive inside an archive).

- **Scan attached files of Office formats**. Scans Microsoft Office files (DOC, DOCX, XLS, PPT and other Microsoft extensions). Office format files include OLE objects as well. The application scans office-format attachments smaller than 1 MB regardless of the state of whether this check box is selected or not.

- **Do not scan archives larger than (MB)**. If this check box is selected, Mail Threat Protection excludes from scanning any attached archives that are larger than the specified limit. If this check box is cleared, Mail Threat Protection scans attached archives of any size.

- **Skip file that is scanned for longer than (sec)**. If this check box is selected, the scan duration for archives attached to email messages is limited.

7. To apply the policy to computers, close the padlock icons and save your changes.

How to optimize attachment scanning on the command line

1. Make sure that the Mail Threat Protection component is enabled:

```
kesl-control --get-task-state 35
```

2. The component must have the `Started` status.

3. If the component is disabled, run the command:

```
kesl-control --start-task 35
```

4. Select an action to perform when a mail threat is detected in incoming messages:

```
kesl-control --set-settings 35 [ScanFileArchive=<Yes|No>] [UseSizeLimit=<Yes|No>] [SizeLimit=<archive size
(MB)>] [UseTimeLimit=<Yes|No>] [TimeLimit=<scan time (sec)>] [ScanFileOffice=<Yes|No>]
```

5. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 35
```

Symbols

Command options

Setting	Description
`ScanFileArchive`	This includes the scanning of ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE and other types of archives. The application identifies archives not just by extension, but also by format. When scanning archives, the application performs recursive unpacking. This makes it possible to detect threats in nested archives (archive inside an archive). By default, the application scans attached archives.
`UseSizeLimit` `SizeLimit`	Limits the size of attached archives that can be scanned. Mail Threat Protection skips an attached archive when scanning if its size exceeds the specified value. By default, the application scans archives of any size.

Setting	Description
`UseTimeLimit` `TimeLimit`	Time limit for scanning attached archives. By default, the scanning time for attached archives is not limited.
`ScanFileOffice`	Scans Microsoft Office files (DOC, DOCX, XLS, PPT and other Microsoft extensions). Office format files include OLE objects as well. The application scans office-format attachments smaller than 1 MB regardless of the state of whether this check box is selected or not. By default, the application scans attached office format files.

What an email attachment filter is for

The attachment filter is not applied to outgoing email messages.

Malicious applications can be distributed in the form of attachments in email messages. You can configure filtering based on the type of message attachments so that files of the specified types are automatically renamed or deleted. By renaming an attachment of a certain type, Kaspersky Endpoint Security can protect your computer against automatic execution of a malicious application.

For example, you can configure attachment filtering for HTML files. An HTML file may contain malicious scripts. If the application renames such a file, the user will not be able to open the HTML page by double-clicking it in an email message. To open the HTML file, the user will need to download the file and rename it. This gives the user time to analyze the received message and prevent the launch of the malicious script.

By default, the application renames files with the CMD, COM, EXE, JS, JSE, MSI, SCR, VBE, VBS, SH extensions. The application replaces the last character of the extension for the specified file types with an underscore character (for example, attachment.doc_).

How to configure the attachment filter in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Communication & Web Protection** → **Mail Threat Protection**.
5. Under **Advanced settings**, select the **Attachment filter** tab.
6. Select the action that the application will take on the email attachment:
   - **Do not modify attachments**. If this option is selected, Mail Threat Protection does not filter files attached to email messages.
   - **Rename attachments of selected types**. If this option is selected, Mail Threat Protection replaces the last character of the extension with an underscore character for specified file types (for example, attachment.doc_). Thus, to open the file, the user needs to rename the file.
   - **Delete attachments of selected types**. If this option is selected, Mail Threat Protection deletes attachments of the specified types from email messages.
7. If at the previous step you selected the **Rename attachments of selected types** or **Delete attachments of selected types** option, select the check boxes for the relevant file types.

8. If the file type that you need is not listed, add a new attachment type:

   a. Click **Add**.

      This opens the form for adding a new attachment type.

   b. In the **Attachment types** field, specify extension masks in the `*.<extension>` (for example, `*.doc`) format.

      If you want to specify more than one file type, enter each file type on a new line.

9. To apply the policy to computers, close the padlock icons and save your changes.

How to configure the attachment filter on the command line

1. Make sure that the Mail Threat Protection component is enabled:

```
kesl-control --get-task-state 35
```

2. The component must have the `Started` status.

3. If the component is disabled, run the command:

```
kesl-control --start-task 35
```

4. Select the action that the application will take on the email attachment:

```
kesl-control --set-settings 35 ExtensionFilter=<Disable|Rename|Delete>
ExtensionMasks.item_#.UseExtensionMask=Yes\
[ExtensionMasks=*.<extention>]
```

5. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 35
```

Symbols

Command options

Setting	Description
`ExtensionFilter`	The action that the application will take on the email attachment: `Disable`. If this option is selected, Mail Threat Protection does not filter files attached to email messages. `Rename` (default). If this option is selected, Mail Threat Protection replaces the last character of the extension with an underscore character for specified file types (for example, attachment.doc_). Thus, to open the file, the user needs to rename the file. `Delete`. If this option is selected, Mail Threat Protection deletes attachments of the specified types from email messages.
`UseExtensionMask=Yes`	Adding a file type to the attachment filter. You can temporarily exclude a file type from the attachment filter instead of removing the file type. To do this, set `ExtensionMasks.item_#.UseExtensionMask=No`
`ExtensionMasks=*.<extention>`	Extension for the attachment type that you want to rename or remove from email messages.

Web Threat Protection

The Web Threat Protection component prevents downloads of malicious files from the internet, and also blocks the connection to malicious and phishing websites. The component provides computer protection with the help of anti-virus databases, the Kaspersky Security Network cloud service, and heuristic analysis.

How Web Threat Protection works

When installing Kaspersky Endpoint Security, the application adds a self-signed certificate, *Kaspersky Anti-Virus Personal Root Certificate*. The application places this certificate in the local trusted certificate store (`/etc/ssl/certs`) and in the certificate store of web browsers. Every time the application starts, it checks if the certificate is present. If the certificate has been deleted, the application restores the certificate automatically.

1. **Interception of an outgoing connection**

   A third party application (such as a browser) initiates a connection to a server. Kaspersky Endpoint Security replaces the server certificate with its own certificate signed with the Kaspersky Anti-Virus Personal Root Certificate. Next, the application intercepts the encryption key and decrypts the communication session. Kaspersky Endpoint Security does this without alerting the user because Kaspersky Anti-Virus Personal Root Certificate is located in the trusted certificate store.

2. **Scanning network traffic**

   Web Threat Protection scans traffic using the following technologies:

   - Anti-virus databases.
   - Cloud services of Kaspersky Security Network.
   - The Heuristic analysis technology allows detecting threats that are not yet covered by Kaspersky databases.

3. **Completion of the scan**

   If a website is classified as malicious or phishing site, Kaspersky Endpoint Security performs the action specified in the Web Threat Protection component settings: it either blocks the connection or displays a warning.

Web Threat Protection settings

1. **Configure the rules of the operating system's firewall**

   If the system has its own network rules or firewalld rules with Drop policies, then for the application to work correctly, you need to add a rule to allow incoming connections from the local device (loopback):

   Example command for iptables:

   ```
   iptables -A INPUT -i lo -j ACCEPT
   ```

2. **Select the network traffic interception mode**

When network packets are received, Web Threat Protection extracts data to scan for threats. The following modes of network traffic interception can be used:

- eBPF
- iptables (default)

The choice of the network traffic interception mode depends on the organization's infrastructure. In a closed perimeter, we recommend using eBPF. In other scenarios, use iptables.

> We recommend grouping devices into different administration groups depending on the network traffic interception mode.

3. **Configure the certificate validation policy**

   By default, Web Threat Protection decrypts and scans network traffic sent over encrypted connections. When doing so, the component can use the internet for the verification and download missing chains required to verify the certificate. If the device does not have direct internet access, you must select a local certificate validation method (without using the internet) or use a proxy server for internet access.

   The certificate validation policy also includes the following settings:

   - Access to websites with an untrusted certificate
   - Access to websites with a certificate validation error

   By default, Kaspersky Endpoint Security allows navigating to a website with an untrusted certificate and adds the domain with a certificate validation error to exclusions. Certificate validation errors can occur, for example, with using banking applications or cloud storage. Domains to which these services belong may reject the Kaspersky Anti-Virus Personal Root Certificate. You can configure your own certificate validation policy.

4. **Add trusted certificates**

   If your organization uses private Certification Authorities to issue certificates for internal servers, Kaspersky Endpoint Security may block access to web resources because of certificate validation errors. Add these certificates to the trusted list to exclude web resources from encrypted connection scanning.

5. **In the Web Threat Protection settings, select the Inform action**

   By default, the Web Threat Protection task is disabled. We recommend enabling Web Threat Protection, and as the action on threat detection, selecting **Inform** and checking access to all corporate resources. Kaspersky Endpoint Security allows access to all websites and logs information about detected threats.

6. **Gather statistics on websites that Web Threat Protection considers unsafe**

   You can get statistics for websites that Web Threat Protection considers unsafe using reports.

7. **Add trusted web addresses**

   After reviewing Web Threat Protection reports, you need to add web addresses that you trust to the trusted list. If the list of trusted web addresses is not sufficient to resolve the conflict of the Kaspersky Endpoint Security application with third-party applications, you can use the special chain of allow rules, kesl_bypass. The *kesl_bypass chain* is a special list of rules that Kaspersky Endpoint Security creates in the mangle table of the operating system firewall (iptables/ip6tables).

8. **In the Web Threat Protection settings, select the Block action**

   Enable the blocking of infected objects in web traffic.

Special considerations and limitations

- The application scans incoming traffic for TCP ports and uses port 9879 on localhost to intercept connections. If port 9879 is in use, the application automatically selects any available port to intercept connections.
- Enabling or disabling the application as well as enabling or disabling the Web Threat Protection and Network Threat Protection components terminates connections on intercepted ports.
- Kaspersky Endpoint Security scans HTTP- and HTTPS-traffic. Kaspersky Endpoint Security scans URLs and IP addresses.
- The application supports the following executable files of browsers, including in snap format:
  - chrome
  - chromium
  - chromium-browser
  - firefox
  - firefox-esr
  - google-chrome
  - opera
  - yandex-browser
- If a user attempts to visit a malicious website, the application does the following:
  - **HTTP**. The application blocks access and displays a warning.
  - **HTTPS**. The application blocks access; the browser displays an error page.
- Removing application certificates may cause the Web Threat Protection component to work incorrectly.

Useful articles

What to do if you get the "Visiting a domain with an untrusted certificate" warning

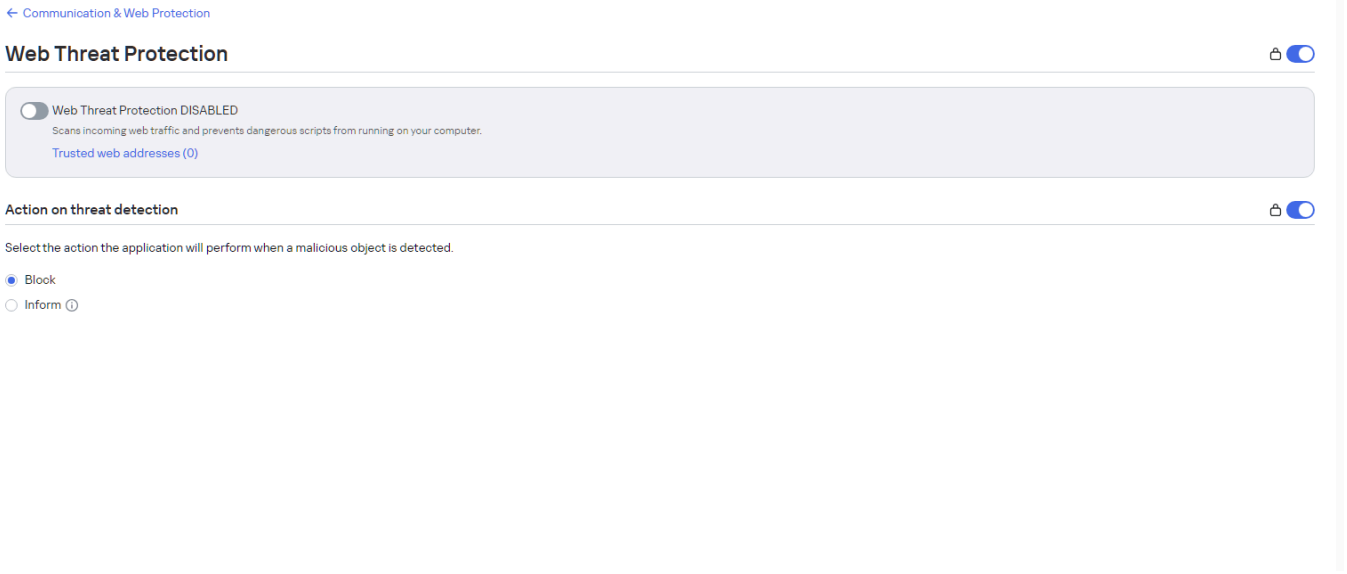
How to select an action on web threat detection

When a web threat is detected, Kaspersky Endpoint Security can block access to dangerous objects or only inform about the detection of a dangerous object.

How to configure actions on web threat detection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Communication & Web Protection** → **Web Threat Protection**.
5. Under **Action on threat detection**, select the action that the application will take when a threat is detected:
   - **Block**. If this option is selected and an infected object is detected in web traffic, the Web Threat Protection component blocks access to the object and displays a message in the browser.
   - **Inform**. Kaspersky Endpoint Security informs the user about the detection of an infected object in web traffic. Web Threat Protection allows this object to be downloaded to the device. At that, the application logs the information about the infected object and adds it to the list of active threats.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Web Threat Protection

How to configure actions on threat detection on the command line

1. Run the following command:

```
kesl-control --set-settings 14 ActionOnDetect=<Block|Notify>
```

2. Select the databases to be used for scanning links:

```
kesl-control --set-settings 14 CheckMalicious=<Yes|No> CheckAdware=<Yes|No> CheckOther=<Yes|No>
```

3. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 14
```

Symbols

Command options

Setting	Description
`ActionOnDetect`	Action on threat detection: • `Block` (default). If this option is selected and an infected object is detected in web traffic, the Web Threat Protection component blocks access to the object and displays a message in the browser. • `Notify`. If this option is selected and an infected object is detected in web traffic, Kaspersky Endpoint Security allows this object to be downloaded to the computer but adds information about the infected object to the list of active threats.
`CheckMalicious`	Scanning the links to determine whether they are included in the database of malicious web addresses allows you to track websites that have been added to denylist. The database of malicious web addresses is maintained by Kaspersky, included in the application installation package, and updated during Kaspersky Endpoint Security database updates. The scan is enabled by default (`Yes`).
`CheckAdware`	Checking links against the database of advertising web addresses. The scan is disabled by default (`No`).
`CheckOther`	Checking links against the database of web addresses containing legitimate applications that intruders can use to compromise the devices or data. The scan is disabled by default (`No`).

What is Anti-Phishing

Web Threat Protection checks links to see if they belong to phishing web addresses. This helps prevent *phishing attacks*. A phishing attack can be disguised, for example, as an email message supposedly from your bank with a link to the official website of the bank. By clicking the link, you go to an exact copy of the bank's website and can even see its real web address in the browser, even though you are on a counterfeit site. From this point forward, all of your actions on the site are tracked and can be used to steal your money.

Because links to phishing websites may be received not only in an email message but also from other sources such as messengers, the Web Threat Protection component monitors attempts to access a phishing website at the web traffic scan level and blocks access to such websites. Lists of phishing URLs are included with the Kaspersky Endpoint Security distribution kit.

You can configure the Anti-Phishing functionality only on the command line. You cannot configure Anti-Phishing in Web Console. By default, Anti-Phishing with heuristic analysis is enabled.

How to enable Anti-Phishing on the command line

1. Make sure that the Web Threat Protection component is enabled:

   ```
   kesl-control --get-task-state 14
   ```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

   ```
   kesl-control --start-task 14
   ```

3. Enable Anti-Phishing:

   ```
   kesl-control --set-settings 14 CheckPhishing=Yes
   ```

4. Configure heuristic analysis for scanning web pages for phishing links:

```
kesl-control --set-settings 14 UseHeuristicForPhishing=<Yes|No>
```

This setting is not applicable to devices with an Elbrus CPU.

5. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 14
```

Network Threat Protection

The *Network Threat Protection* component (also called Intrusion Detection System, IDS) monitors inbound network traffic for activity characteristic of network attacks. When the application detects an attempted network attack on a user's computer, it blocks the network connection with the attacking computer. Descriptions of currently known types of network attacks and ways to counteract them are provided in the application databases. The list of network attacks that the Network Threat Protection component detects is updated during database and application module updates.

How Network Threat Protection works

1. **The application analyzes incoming packets**

   To scan incoming traffic, the Network Threat Protection component receives port numbers from the application databases and accepts connections via all these ports. During the network scan process in the iptables traffic interception mode, it may look like an open port on the device, even if no application on the system is listening to this port. We recommend closing unused ports by means of a firewall.

2. **The application scans incoming traffic**

   Network Threat Protection scans incoming traffic using the following technologies:

   - Anti-virus databases.
   - Cloud services of Kaspersky Security Network.
   - The Heuristic analysis technology allows detecting threats that are not yet covered by Kaspersky databases.

3. **Completion of the scan**

   When a network threat is detected, the application blocks all network connections from the attacking device for a specified time.

Network Threat Protection settings

1. **Configure the rules of the operating system's firewall**

   To ensure compatibility of REDIRECT rules (for example, redirection from port 443 to 8443) with interception rules of Network Threat Protection, you need to delete the REDIRECT rules and add interception rules.

   Example of a command to delete REDIRECT rules:

   ```
   iptables -t nat -D PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

   Example of commands for adding interception rules:

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
   ```

   ```
   iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT -
   -to-destination :8443
   ```

2. **Create a list of monitored network ports**

   By default, the application monitors known and registered ports, for example, port 443 for HTTPS connections, port 143 for the IMAP mail protocol. Default settings provide recommended protection level and optimal resource use. If necessary, you can change the list of monitored ports or enable monitoring of all ports.

3. **Select the traffic interception mode**

   When network packets are received, Network Threat Protection extracts data to scan for threats. The following modes of incoming traffic interception can be used:

   - eBPF
   - iptables (default)

   The choice of the traffic interception mode depends on the infrastructure of the organization. In a closed perimeter, we recommend using eBPF. In other scenarios, use iptables.

   > We recommend grouping devices into different administration groups depending on the traffic interception mode.

4. **Enable Web Threat Protection in Inform mode**

   By default, Network Threat Protection is disabled. Before enabling Network Threat Protection in Block mode, we recommend enabling the component in Inform mode. This lets Kaspersky Endpoint Security detect suspicious network activity and log information about detected network attacks without disrupting network connections. Check the access of third-party corporate applications to network resources. Make sure that network ports control does not does not slow down these applications.

5. **Collect statistics for IP addresses from which Network Threat Protection observes suspicious network activity**

   You can review reports to get statistics for IP addresses that Network Threat Protection considers unsafe. The application generates *Network attack detected* events.

6. **Add trusted IP addresses**

   After reviewing Network Threat Protection reports, you need to add the IP addresses of devices whose network connections you trust to the trusted list. You can add the address of an individual device or subnet to the list of exclusions. Network Threat Protection will not intercept or scan packets coming from such a device.

7. **Enable Network Threat Protection in Block mode**

   After adding the IP addresses of trusted devices to the list of exclusions, enable the component in Block mode. Network activity of untrusted devices is blocked, and information to that effect appears in reports.

Special considerations and limitations

- The application scans incoming traffic for TCP ports. The application uses fixed port 9789 on localhost to intercept connections.
- Enabling or disabling the application as well as enabling or disabling the Web Threat Protection and Network Threat Protection components terminates connections on intercepted ports.
- Network Threat Protection does not work on computers running CentOS 5.2 and 5.4 due to the lack of TProxy support.

How to select an action on network threat detection

If an attempted network attack on a protected device is detected, the application blocks network activity from the attacking device and creates a *Network attack detected* event.

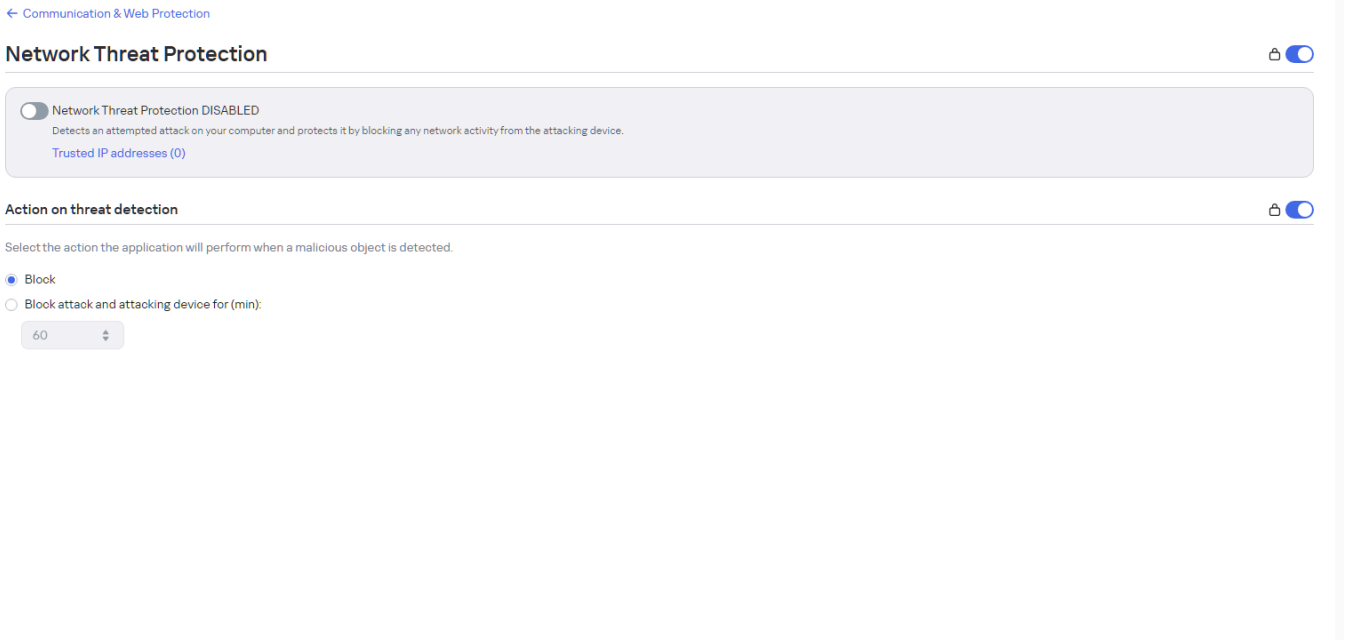
To block network traffic, Kaspersky Endpoint Security creates a dynamic firewall rule. The firewall temporarily blocks network traffic for the attacking device. The application also adds the compromised device to the list of blocked devices. Access to shared network directories is denied to blocked devices.

How to configure actions on network attack detection in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Communication & Web Protection** → **Network Threat Protection**.
5. Make sure the toggle switch for the component is in the **Network Threat Protection ENABLED** position.
6. Select the **Enable Network Threat Protection for Linux devices** check box.
7. Under **Action on threat detection**, select the action that the application will take when a threat is detected: **Block** or **Block attack and attacking device for (min)**.
8. If **Block attack and attacking device for (min)** is selected, set the blocking duration of the compromised device in minutes. By default, the device is blocked for 60 minutes. Valid values are 1 to 999.

9. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Network Threat Protection

How to configure actions on network attack detection on the command line

1. Make sure that the Network Threat Protection component is enabled:

   ```
   kesl-control --get-task-state 17
   ```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

   ```
   kesl-control --start-task 17
   ```

3. Select an action on network threat detection:

   ```
   kesl-control --set-settings 17 ActionOnDetect=<Block|Notify>
   ```

4. Configure blocking of the compromised device:

   ```
   kesl-control --set-settings 17 BlockAttackingHosts=<Yes|No>
   ```

5. Select the blocking period for the `BlockAttackingHosts=Yes` action:

   ```
   kesl-control --set-settings 17 BlockDurationMinutes=<Blocking period>
   ```

6. To check the current values of the component settings, run the following command:

   ```
   kesl-control --get-settings 17
   ```

Symbols

Command options

Setting	Description
`ActionOnDetect`	Action on network threat detection: • `Block` (default) blocks network traffic for the compromised device and creates a *Network attack detected* event. • `Notify` creates a *Network attack detected* event without blocking network traffic.
`BlockAttackingHosts`	Block the network activity of the attacking device. By default, device blocking is enabled.
`BlockDurationMinutes`	Configure the blocking duration of the remote device that is involved in malicious activity or malicious data encryption.

How to manage blocked devices

While protecting a device against network threats and remote malicious encryption, Kaspersky Endpoint Security can block remote devices whose actions are considered to be malicious. Devices are protected against threats of these types by the Anti-Cryptor and Network Threat Protection components. Kaspersky Endpoint Security blocks network traffic for a certain length of time. When the blocking period expires, Kaspersky Endpoint Security allows the network traffic to resume. By default, the application blocks network traffic for an attacking device for 60 minutes. When the blocking time expires, the application removes this device from the list of blocked devices.

If Kaspersky Endpoint Security has blocked a trusted device, you need to add IP address of this device to the list of exclusions.

How to view the list of blocked devices

```
kesl-control -H --get-blocked-hosts
```

As a result of the command execution, the application outputs the list of blocked devices to the console.

List of blocked devices

```
Blocked devices: 1
Host                : 10.69.119.234
Block date          : 2026-04-29 15:44
Will be unblocked   : 2026-04-29 16:44
Task name           : Network_Threat_Protection
```

How to unblock a device

```
kesl-control -H --allow-hosts <address>
```

Where `<address>` is one or more IP addresses of the devices or subnets (IPv4/IPv6, including addresses in short form). You can specify multiple IP addresses of devices or subnets by separating them with a space.

Firewall Management

The operating system's firewall controls all network activity of the device, be it activity on the internet or the local network. The firewall protects the data on the device from unauthorized access and blocks most threats, for example, attacks on the device coming from the network. The firewall allows detecting all network connections on the user device and getting a list of their IP addresses.

The application manages the operating system's firewall using the Firewall Management component. The component adds network packet rules to the firewall of the operating system to monitor the network activity of devices. You can use network packet rules to specify the desired level of device protection, from fully blocking Internet access for all applications to allowing unlimited access.

The Firewall Management component is disabled by default.

When the Firewall Management component is enabled, Kaspersky Endpoint Security automatically deletes all custom rules configured for the firewall with tools provided by the operating system. These rules are not restored after the component is disabled.

If Firewall Management is enabled, Kaspersky Endpoint Security checks the operating system's firewall every 60 seconds. If the check finds that a third-party application or utility has added or removed a network packet rule, Kaspersky Endpoint Security restores the set of firewall rules created using the application.

Kaspersky Endpoint Security still scans the operating system firewall when firewall management is disabled. This allows the application to restore dynamic rules.

Before enabling the Firewall Management component, perform the following actions:

- Disable other tools that manage the operating system's firewall.
- Save and back up any custom firewall rules configured before enabling the Firewall Management component.

How to create a network packet rule

The firewall filters all network activity on the protected devices in accordance with *network packet rules*. Network packet rules restrict network packets or connections regardless of the application. Rules allow or deny network activity in accordance with the following conditions:

- Connection protocol and port
- Traffic direction
- IP address of the device that is sending or receiving network traffic

Priorities of network packet rules

By default, all outgoing packets and connections. Default rules have the lowest priority: if no other network packet rule has been triggered or if no other network packet rules have been specified, the activity is allowed.

The firewall applies network packet rules in the order of their priority. The priority of a rule is its position in the list, from top to bottom. The firewall filters a network connection by the first rule in the list and either allows or blocks network activity. If the rule does not match, the firewall applies the next rule and so on down the list. The component then ignores all network packet rules after the matched rule for the connection.

Recommendations for creating network packet rules

To create network packet rules on the command line, you can use command line options or a configuration file. If you want to add multiple rules, use a configuration file to add them.

Adding a large number of rules one at a time using command line options may cause the CPU load to spike.

How to create a network packet rule in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Communication & Web Protection** → **Firewall**.
5. Make sure the toggle switch for the component is in the **Firewall ENABLED** position.
6. On the **Network packet rules** tab, click the **Add** button.

   This opens the new network rule form (see the figure below).
7. In the **Rule name** field, enter the name of the rule.

   You can select a predefined rule template by clicking the **Select rule template** link. Rule templates contain settings for the most frequently used network connections.

   All settings of a network rule, except for the priority and actions that the firewall applies to the connection are filled in automatically.
8. In the **Priority** field, specify the priority of the rule. By default, a rule is created with the highest priority.
9. Under **Action**, select how you want the firewall to process network activity when the rule is triggered: **Allow** or **Block**.
10. In the **Direction** field, select which network activity you want the rule to apply to:

    - **Inbound**. Firewall applies the network rule to all inbound network packets.
    - **Inbound (packet)**. Firewall applies the network rule to all network packets sent via a connection that was initiated by a remote computer.
    - **Inbound / Outbound**. Firewall applies the network rule to both inbound and outbound network packets, regardless of whether the user's computer or a remote computer initiated the network connection.
    - **Outbound (packet)**. Firewall applies the network rule to all outbound network packets.
    - **Outbound**. Firewall applies the network rule to all network packets sent via a connection that was initiated by the user's computer.
    - **Inbound / Outbound (packets)**. Firewall applies the network rule to all inbound and outbound network packets.

11. If you want the actions of the network rule to be reflected in the report, select the **Log events** check box. In accordance with the action of the rule, the application creates a *Network activity blocked* or *Network activity allowed* event.

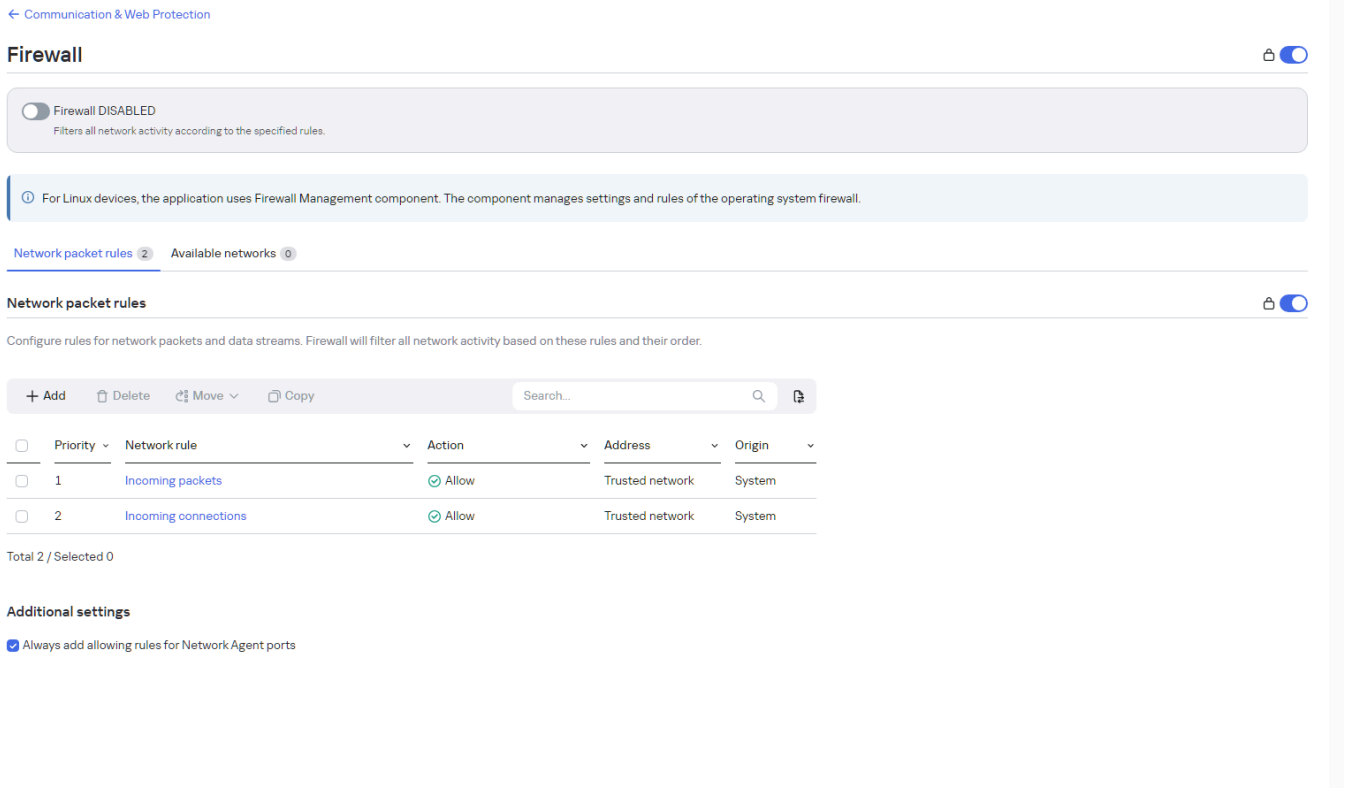
12. On the **Protocol settings** tab, select the protocol for which you want the rule to filter network activity.

13. Go to the **Remote network addresses** tab.

14. In the **Remote** field, specify the network addresses of the remote computers that can send and receive network packets: The firewall will apply the rule to the specified addresses.

15. In the **Local** field, specify the network addresses of the computers with Kaspersky Endpoint Security installed that can send and receive network packets: The firewall will apply the rule to the specified addresses.

16. To apply the policy to computers, close the padlock icons and save your changes.



Firewall

How to create a network packet rule on the command line

1. Make sure that Firewall Management is enabled:

```
kesl-control --get-task-state 12
```

The component must have the **Started** status.

2. If the component is disabled, run the command:

```
kesl-control --start-task 12
```

3. Add a new network packet rule:

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
```

```
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

If you want to add multiple rules, use a configuration file to add them:

a. Output the settings of the component to the configuration file:

```
kesl-control --get-settings 12 --file <path to file> [--json]
```

b. Open the configuration file and add network packet rules with the following sections:

```
[PacketRules.item_#]
Name=<rule name>
FirewallAction=<Allow|Block>
Protocol=<protocol>
Direction=<direction>
RemoteAddress=<remote address>
LocalAddress=<local address>
LogAttempts=<Yes|No>
```

c. Import the settings from the configuration file into the application:

```
kesl-control --set-settings 12 --file <path to file> [--json]
```

4. To view the list of network packet rules, run the following command:

```
kesl-control -F --query
```

The application displays a list of all network packet rules in the following format: `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`.

Symbols

Command options

Setting	Description
`--name <rule name>` `Name`	Network packet rule name. By default, `Packet rule #<n>`.
`--action` `FirewallAction`	Action to be performed on connections specified in this network packet rule. • `Allow` (default) to allow connections. • `Block` to block connections.
`--protocol` `Protocol`	Type of protocol for which you want to monitor network activity. • `Any` (default) means that the firewall controls all network activity • `TCP` • `UDP` • `ICMP` • `ICMPv6` • `IGMP` • `GRE`

Setting	Description
`--direction` `Direction`	Direction of the monitored network activity: • `IncomingOutgoing` or `InOut` (default). Firewall applies the network rule to all inbound and outbound network packets. • `Incoming` or `In`. Firewall applies the network rule to all network packets sent via a connection that was initiated by a remote computer. • `Outgoing` or `Out`. Firewall applies the network rule to all network packets sent via a connection that was initiated by the user's computer. • `IncomingPacket` or `InPacket`. Firewall applies the network rule to all inbound network packets. • `OutgoingPacket` or `OutPacket`. Firewall applies the network rule to all outbound network packets. • `IncomingOutgoingPacket` or `InOutPacket`. Firewall applies the network rule to both inbound and outbound network packets, regardless of whether the user's computer or a remote computer initiated the network connection.
`--remote <remote address[:<port>]>` `RemoteAddress=<remote address>`	IP address of the remote device: • `Any` (default) enables monitoring of network packets sent and/or received by remote devices with any IP address. • `Trusted` is the configured network zone for trusted networks. • `Local` is the configured network zone for local networks. • `Public` is the configured network zone for public networks. • `d.d.d.d` is the IPv4 address, where d is a decimal number from 0 to 255. • `d.d.d.d – d.d.d.d` is a range of IPv4 addresses. • `d.d.d.d/p` is an IPv4 subnet, where `p` is a number from 0 to 32. • `x:x:x:x:x:x:x:x` is an IPv6 address, where x is a hexadecimal number from 0 to ffff. • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` is a range of IPv6 addresses. • `x:x:x:x:x:x:x:x/p` is the subnet of IPv6 addresses, where `p` is a number from 0 to 128; you can use `::` for brevity. You can also specify a remote port: • `Any` (default) to monitor all remote ports • `0 – 65535`.
`--local <local address[:<port>]>` `LocalAddress=<local address>`	Network address of a device with Kaspersky Endpoint Security installed: • `Any` (default) to monitor network packets sent and/or received by local devices with any IP address. • `Trusted` is the configured network zone for trusted networks. • `Local` is the configured network zone for local networks. • `Public` is the configured network zone for public networks. • `d.d.d.d` is the IPv4 address, where d is a decimal number from 0 to 255. • `d.d.d.d – d.d.d.d` is a range of IPv4 addresses. • `d.d.d.d/p` is an IPv4 subnet, where `p` is a number from 0 to 32. • `x:x:x:x:x:x:x:x` is an IPv6 address, where x is a hexadecimal number from 0 to ffff. • `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` is a range of IPv6 addresses. • `x:x:x:x:x:x:x:x/p` is the subnet of IPv6 addresses, where `p` is a number from 0 to 128; you can use `::` for brevity. You can also specify a local port: • `Any` (default) to monitor all local ports • `0 – 65535`.
`--at <index>`	Index of the rule in the list of network packet rules. If the `--at` option is not specified or its value is larger than the number of rules in the list, the new rule is added to the end of the list.
`LogAttempts`	Include a record of the network rule action in the report. • `Yes` — Log actions in the report. • `No` (default value)—Do not write the actions in the report.

Example of a rule that blocks all incoming and established connections to TCP port 23

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote any
```

Example of a rule that blocks incoming and established connections via the TCP port 23 for the Public network zone

```
kesl-control -F --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --
remote Public
```

Network packet rule usage examples

1. **Allow internet access to only one specific computer on the local network, and block access for all others**

   Rule for a computer (192.168.2.22) that is allowed to access the internet via the TCP protocol:

   ```
   kesl-control --add-rule --name InternetAccess --action Allow --protocol TCP --local 192.168.2.22
   ```

   Rule for other computers for which internet access is blocked:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.1.0/24
   ```

2. **Block internet access for only one specific computer on the local network**

   Rule for the computer (192.168.2.23) for which internet access is blocked:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.23
   ```

3. **Block access to a specific website from the local network**

   Rule for computers on the local network that are denied HTTP access to example.com (91.198.174.192):

   ```
   kesl-control --add-rule --name ExampleHTTP --action Block --protocol TCP --remote 91.198.174.192:80
   ```

   Rule for computers on the local network that are denied HTTPS access to example.com (91.198.174.192):

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Block --protocol TCP --remote 91.198.174.192:443
   ```

4. **Allow access to only one specified website to a specific computer on the local network**

   Rule for a computer (192.168.2.24) that is allowed HTTP access to example.com (91.198.174.192):

   ```
   kesl-control --add-rule --name ExampleHTTP --action Allow --protocol TCP --remote 91.198.174.192:80 --local
   192.168.2.24
   ```

   Rule for a computer (192.168.2.25) that is allowed HTTPS access to example.com (91.198.174.192):

   ```
   kesl-control --add-rule --name ExampleHTTPS --action Allow --protocol TCP --remote 91.198.174.192:443 --local
   192.168.2.25
   ```

   Rule for the computer (192.168.2.26), which blocks internet access:

   ```
   kesl-control --add-rule --name InternetBlock --action Block --protocol TCP --local 192.168.2.26
   ```

How to add an IP address to a network zone: Public, Local, Trusted

The firewall allows monitoring network activity for *network zones*. A network zone is a group of IP addresses or subnets that are grouped together under one type of network connection. You can use a predefined network zone to reuse a rule for multiple IP addresses or subnets without having to create a separate rule for each IP address or subnet.

Kaspersky Endpoint Security distinguishes three network zones:

- **Public network**. The network is not protected by antivirus applications, firewalls, or filters (such as Wi-Fi in a cafe). When the user operates a computer that is connected to such a network, the firewall blocks access to files and printers of this computer. External users are also unable to access data through shared folders and remote access to the desktop of this computer.
- **Local network**. Network for users with restricted access to files and printers on this computer (such as for a corporate LAN or home network).
- **Trusted network**. Safe network in which a computer is not exposed to attacks or unauthorized data access attempts. The firewall permits any network activity within networks with this status.

How to add an IP address to a network zone in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Communication & Web Protection** → **Firewall**.
5. Go to the **Available networks** tab.
6. Click **Add**.

   This opens the form for adding a new network connection.
7. In the **Name** field, enter the name of the network connection.
8. In the **Network type** field, select the network zone to which the network connection belongs: **Public network**, **Local network**, **Trusted network**.
9. In the **IP address** field, specify the IP address or subnet that will be associated with the network connection.
10. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to add an IP address to a network zone on the command line

1. Make sure that Firewall Management is enabled:

   ```
   kesl-control --get-task-state 12
   ```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

```
kesl-control --start-task 12
```

3. Add the address to the network zone:

```
kesl-control -F --add-zone <Public|Local|Trusted> --address <IP address>
```

To view the list of network packet rules, run the following command:

```
kesl-control -F --query
```

Symbols

Command options

Setting	Description
`--add-zone`	Predefined network zone: • `Public`. Public network. • `Local`. Local network. • `Trusted`. Trusted network.
`--address`	Network address or subnet.

Example

```
kesl-control -F --add-zone Local --address 10.28.0.0/24
```

What are dynamic rules

Kaspersky Endpoint Security allows adding or removing firewall *dynamic rules* that the application needs to work correctly. For example:

- Network Agent adds dynamic rules that allow connecting to Kaspersky Security Center.
- The Anti-Cryptor component adds dynamic rules for intercepting traffic transmitted via the NFS and SMB file transmission and storage protocols. This allows the component to block network traffic for devices whose actions the application interprets as malicious encryption.
- If Kaspersky Endpoint Security is used in Light Agent mode, dynamic rules are automatically added to the firewall that allow connections to the SVM and Integration Server.

Kaspersky Endpoint Security automatically creates dynamic rules that allow application components to access network resources. Dynamic rules do not depend on the Firewall Management component state (enabled/disabled) or changes to the settings of the component operation. The execution priority of dynamic rules is higher than the priority of network packet rules. The application restores a set of dynamic rules if any of them are deleted, for example, by using the iptables utility. If the kesl process is killed by the Watchdog server, all links to the rule chains created by the application while it was working (except for kesl-bypass) are deleted from iptables.

You can view the set of dynamic rules using the following command:

```
kesl-control -F --query
```

The application displays a list of all network packet rules in the following format: `<IP protocol version> <table> <chain> <rule in the format of the iptables-save utility>`. Dynamic rules are segregated into separate chains: `kesl_input`, `kesl_output`, `kesl_prerouting`, `kesl_postrouting`, `kesl_forward`.

You cannot manage the settings of dynamic rules.

Example

```
ipv4 mangle kesl_output -p tcp -m tcp --dport 80 -m mark ! --mark 0x400/0x400 -m conntrack --ctdir ORIGINAL -m
addrtype ! --dst-type LOCAL -j MARK --set-xmark 0x100/0x100 tag WebAv
```

How to create rules for connecting to Kaspersky Security Center

Network Agent is used for interaction with Kaspersky Security Center. For a permanent connection between Network Agent and Kaspersky Security Center, you need to add allow rules for Network Agent's ports. In this case, even if you configure the firewall incorrectly and accidentally block all connections, you will be able to remotely configure the firewall in the Kaspersky Security Center console.

The set of ports depends on the computer's role (for example, distribution point). To learn more about the ports that will be opened on the computer, refer to the Kaspersky Security Center Help.

How to add allow rules for Network Agent in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Select **Communication & Web Protection** → **Firewall**.
5. Make sure the toggle switch for the component is in the **Firewall ENABLED** position.
6. Select the **Always add allowing rules for Network Agent ports** check box.
7. To apply the policy to computers, close the padlock icons and save your changes.

How to add allow rules for Network Agent on the command line

1. Make sure that Firewall Management is enabled:

   ```
   kesl-control --get-task-state 12
   ```

   The component must have the **Started** status.
2. If the component is disabled, run the command:

   ```
   kesl-control --start-task 12
   ```

3. Run the following command:

```
kesl-control --set-settings 12 OpenNagentPorts=Yes
```

4. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 12
```

Security Controls

Device Control

Device Control manages user access to devices that are installed on or connected to the client device (for example, hard drives, cameras, or Wi-Fi modules). This lets you protect the client device from infection when external devices are connected, and prevent data loss or leaks.

How Device Control works

By default, the Device Control component is enabled with default settings.

1. **A user tries to gain access to the device**
2. **Device Control manages user access on the following levels:**
   - **Device type** as classified by Device Control, such as printers, removable drives, or CD/DVD drives. One of the following *access modes* can be applied to each device type:
     - *Allow*, to allow access to devices of this type.
     - *Block*: block access to devices of this type.
     - *Depends on bus*: allow or block access to devices depending on the access mode set for the bus through which the device is connected.
     - *Custom*: allow or block access to devices depending on the device access rules.
     - *Read only*: allow read-only access to devices of the selected type, while blocking write access.
   - **Connection bus**. *Connection bus* is an interface that devices use to connect to the client device, such as USB or FireWire. One of the following access modes can be applied to connection buses:
     - *Allow*: grant access to devices connected through this connection bus.
     - *Block*: deny access to devices connected using this connection bus.

   For example, access may be denied to all devices connected via USB.

3. **Completion of the scan**

   If the device to which the user is trying to gain access is not a trusted device for this user, or the user does not have permission to gain access to the device in accordance with the access mode, the application blocks access to the device for this user.

   The user can send a request to the organization's administrator to complain about mistaken blocking if the user believes this is the case, or the user can request temporary access to the device.

When Device Control is disabled, the application unblocks access to blocked devices.

Configuring Device Control

1. **Configure trusted devices**

   Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times. You can grant access to trusted devices to an individual user, a group of users, or all users of the organization. For example, you can limit access to specific USB devices or only to USB drives; access to other USB devices is denied.

2. **Configure access mode**

   You can configure access mode for device types and connection buses. By default, the *Depends on bus* access mode is selected for all device types. The *Allow* access mode is selected for connection buses. Device Control grants users full access to all devices accordingly.

3. **Configure access rules**

   For storage devices (hard drives, removable drives, floppy disk drives, and CD/DVD drives), you can configure *access rules*.

4. **Configure the message template**

   If necessary, you can customize the template text of the message that notifies the user about blocked access to the device or a prohibited operation with the device.

5. **Configure temporary access to the device**

   If necessary, allow users to gain temporary access to a blocked device.

Special considerations and limitations

- When Device Control is enabled for the first time, it generates a *DeviceAllowed* event for all detected devices with a known device or bus type. No repeat events are generated upon subsequent component runs unless there were changes in the control settings for these devices.

- Device Control does not block system drives. If the application cannot automatically detect the system drive, the Device Control component terminates with an error.

- Blocking devices by device type or connection bus via the system device driver is not supported on the following Linux kernels: 3.10, 5.14, 5.15, 5.17, 6.1, 6.8. On these kernels and in the *By rule* access mode, only the opening of files and reading of directories (that is, getting the names of files and directories) are blocked. On systems that do not support fanotify, blocking the reading of directories is also not supported.

- Device Control ignores mount point exclusions. Access to a device mounted at an excluded point can be limited with Device Control settings.

- In general application settings, if blocking access to files during scans is disabled, you cannot use a device access schedule to block access to devices.

How to manage the list of trusted devices on the command line

The list of trusted devices contains information about devices that are allowed to be accessed (for specific users or groups).

In the command line, you can view the list of trusted devices, add and remove devices from the list, and import the list of trusted devices from a file.

```
View the list of trusted devices
kesl-control --trusted-devices --list
```

```
Add a device to the list of trusted devices
kesl-control --trusted-devices --add <device id or mask>
```

where `<device id or mask>` is the device ID or device ID mask.

```
Delete a device from the list of trusted devices
kesl-control --trusted-devices --delete <device id or mask>
```

where `<device id or mask>` is the device ID or device ID mask.

```
Import the list of trusted devices from a file
kesl-control --trusted-devices --merge|--add|--replace --file <file>
```

where:

- `--merge` merges the lists of trusted devices. If the current list and the imported list contain entries for a device with the same ID, the existing entries are updated. For devices that are not in the current list, entries are added.

- `--add` adds the current list of trusted devices when importing. Only entries for devices not previously on the list of devices are added to the list.

- `--replace` replaces the current list of trusted devices. The existing list of trusted devices is replaced with the imported list.

- `--file <file>` is the full path to the JSON file that the list of trusted devices will be imported from.

How to configure device access mode

For each device type (according to the classification of the Device Control component, for example, printers, removable drives, CD / DVD drives), one of the following *access modes* can be applied:

- *Allow*, to allow access to devices of this type.
- *Block*: block access to devices of this type.
- *Depends on bus*: allow or block access to devices depending on the access mode set for the bus through which the device is connected.
- *Custom*: allow or block access to devices depending on the device access rules. A *device access rule* is a set of options that determine which users can access devices that are installed on the client device or connected to it, and at what time. This access mode can be specified only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives).
- *Read only*: allow read-only access to devices of the selected type, while blocking write access. This access mode can be specified only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives). If the device has the "Read-only" access type, when the trusted device is assigned to a specific user, the assigned user is ignored and the device is made available for writing to all users.

How to configure device access mode for device types in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **Device Control**.
5. Make sure the toggle switch for the component is in the **Device Control ENABLED** position.
6. Under **Device access rules**, in the table, select the **Devices and Wi-Fi networks** tab.
7. In the **Name** column, select the device type for which you want to configure the access mode.
8. In the **Access** drop-down list, select one of the following access modes:
   - **Allow**: allow access to devices of the selected type.
   - **Block**: prohibit access to devices of the selected type.
   - **Depends on bus** (default value): allow or block access to the devices depending on the access mode for a connection bus.
   - **Custom**: allow or block access to devices depending on the access rule and schedule. This option is available only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives).
   - **Read only**: allow read-only access to devices of the selected type. This option is available only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives).

9. In the table below, click the **Add** button.

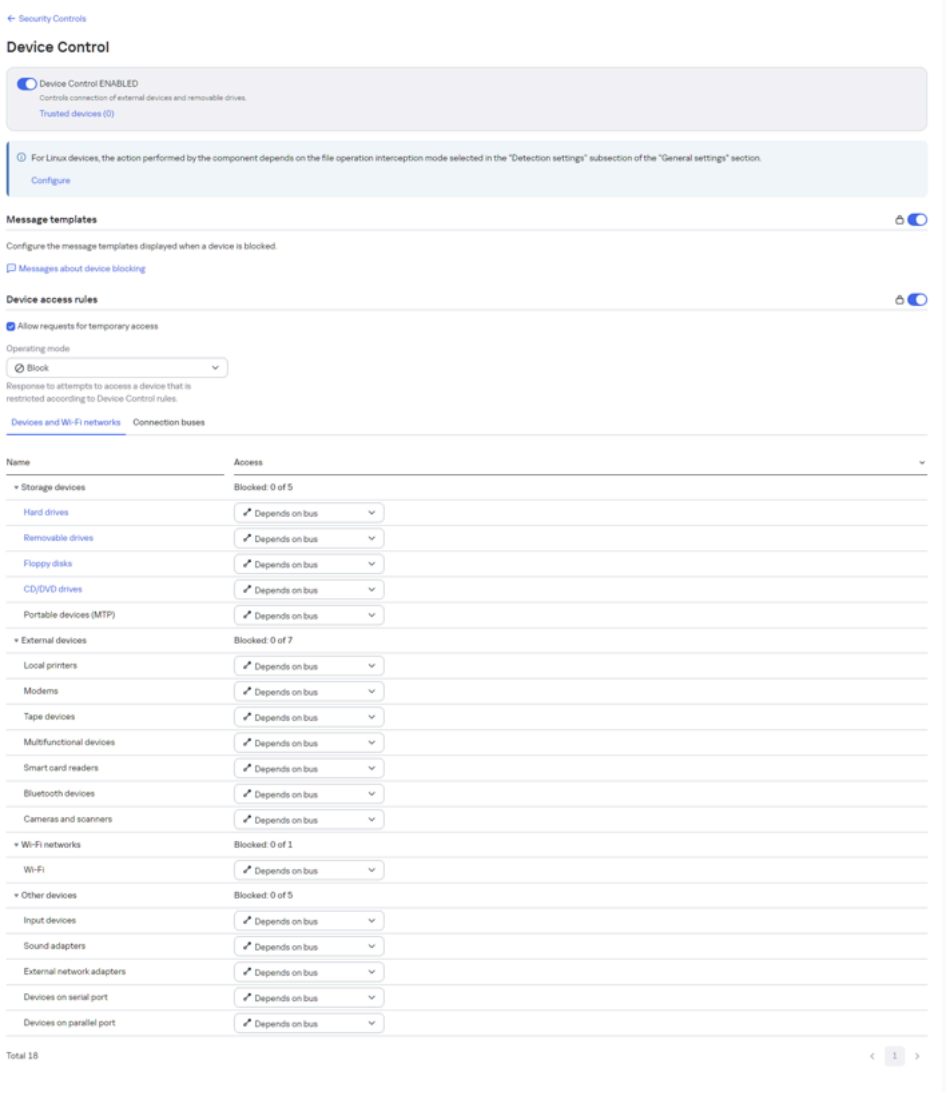
   This opens a window for adding a new access rule.

10. In the **Priority** field, set the access rule priority.

11. Select the users or user group to which the access rule will apply. By default, the rule applies to all users.

12. If necessary, set an access schedule. By default, the rule is always applied.

13. To apply the policy to computers, close the padlock icons and save your changes.



Device Control

How to configure device access mode for device types on the command line

1. Make sure that the Device Control component is running:

   ```
   kesl-control --get-task-list
   ```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

   ```
   kesl-control --start-task 15
   ```

3. Select the operating mode when attempting to access a device that is restricted according to Device Control rules:

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. Specify the access mode for one of the device types: `HardDrive`, `RemovableDrive`, `FloppyDrive`, `OpticalDrive`, `SerialPortDevice`, `ParallelPortDevice`, `Printer`, `Modem`, `TapeDrive`, `MultifuncDevice`, `SmartCardReader`, `WiFiAdapter`, `NetworkAdapter`, `PortableDevice`, `PortableDevice`, `BluetoothDevice`, `ImagingDevice`, `SoundAdapter`, `InputDevice`

```
kesl-control --set-settings 15 DeviceClass.<device type>=<Allow|Block>
```

5. To view Device Control settings, run the following command:

```
kesl-control --get-settings 15
```

How to configure the connection bus access mode in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **Device Control**.
5. Make sure the toggle switch for the component is in the **Device Control ENABLED** position.
6. Under **Device access rules**, in the table, select the **Connection buses** tab.
7. In the **Name** column, select the bus for which you want to configure the access mode.
8. In the **Access** drop-down list, select one of the following access modes:
   - **Allow**: grant access to devices connected through this connection bus.
   - **Block**: deny access to devices connected using this connection bus.
9. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to configure connection bus access mode on the command line

1. Make sure that the Device Control component is running:

```
kesl-control --get-task-list
```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

```
kesl-control --start-task 15
```

3. Select the operating mode when attempting to access a device that is restricted according to Device Control rules:

```
kesl-control --set-settings 15 OperationMode=<Notify|Block>
```

4. Specify access mode for connection buses:

```
kesl-control --set-settings 15 DeviceBus.USB=<Allow|Block>
kesl-control --set-settings 15 DeviceBus.FireWire=<Allow|Block>
```

5. To view Device Control settings, run the following command:

```
kesl-control --get-settings 15
```

How to configure device access rules

For storage devices (hard drives, removable drives, floppy disk drives, and CD/DVD drives), you can configure access rules. *A device access rule* is a set of options that determine which users can access devices that are installed on the client device or connected to it, and at what time. This access mode can be specified only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives). When a forbidden device is connected, the application denies access to the device to the users specified in the rule and displays a notification. During attempts to read and write on this device, the application silently blocks the users specified in the rule from reading/writing. If you try to perform an operation with a device whose access mode is set to *By rule*, but no rule active at the time of access is found, the operation is blocked.

How to configure a device access rule in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **Device Control**.
5. Make sure the toggle switch for the component is in the **Device Control ENABLED** position.
6. Under **Device access rules**, in the table, select the **Devices and Wi-Fi networks** tab.
7. In the **Name** column select the type of storage device for which you want to add an access rule (hard drives, removable drives, floppy drives, CD / DVD drives).
8. In the window that opens, under **Device access rules**, select **Custom**.

9. In the table below, click the **Add** button.

   This opens a window for adding a new access rule.

10. In the **Priority** field, set the access rule priority.

11. Select the users or user group to which the access rule will apply. By default, the rule applies to all users.

12. If necessary, set an access schedule. By default, the rule is always applied.

13. To apply the policy to computers, close the padlock icons and save your changes.

How to configure a device access rule on the command line

1. Make sure that the Device Control component is running:

   ```
   kesl-control --get-task-list
   ```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

   ```
   kesl-control --start-task 15
   ```

3. To view Device Control settings, run the following command:

   ```
   kesl-control --get-settings 15
   ```

4. Select the operating mode when attempting to access a device that is restricted according to Device Control rules:

   ```
   kesl-control --set-settings 15 OperationMode=<Notify|Block>
   ```

5. Add a new access rule for one of the device types: `HardDrivePrincipals.item_#.AccessRules.item_#`, `RemovableDrivePrincipals.item_#.AccessRules.item_#`, `FloppyDrivePrincipals.item_#.AccessRules.item_#`, or `OpticalDrivePrincipals.item_#.AccessRules.item_#`.

   - Enable the rule and specify the default schedule:

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.UseRule=Yes
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.ScheduleName=Default
     ```

     Example

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - Set the Device Control action when the rule is triggered:

     ```
     kesl-control --set-settings 15
     <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.AccessRules.item_#.Access=Allow|Block
     ```

     Example

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.AccessRules.item_0001.UseRule=Yes
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.Access=Allow
     RemovableDrivePrincipals.item_0001.AccessRules.item_0001.ScheduleName=Default
     ```

   - If necessary, specify the users to which the rule will apply:

     ```
     kesl-control --set-settings 15 <Hard|Removable|Floppy|Optical>DrivePrincipals.item_#.Principal=<Name>=
     <\Everyone|user name|@group name>
     ```

     Example

     ```
     kesl-control --set-settings 15 RemovableDrivePrincipals.item_0001.Principal=\Everyone
     ```

   - If necessary, edit the rule schedule:

     ```
     kesl-control --set-settings 15 Schedules.item_#.ScheduleName=<Name> Schedules.item_#.DaysHours=<All|day of
     the week|hour>
     ```

     Example

     ```
     kesl-control --set-settings 15 Schedules.item_0001.ScheduleName=Default Schedules.item_0001.DaysHours=All
     ```

How to configuring the Device Control message template

When a user tries to gain access to a blocked device, the application displays a message about access denial or the blocking of an operation with the device.

Access denial messages are based on a template that describes the reasons for blocking. You can use special variables (for example,%USER_NAME%) in the message template. Such variables allow using the same message template for different devices. When generating a message, the application substitutes the values of variables corresponding to the specific device, user, and event into the message.

You can edit the message template.

How to edit the message template in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **Device Control**.
5. Under **Message templates**, click the **Messages about device blocking** link.

   This opens the message template configuration window.
6. Configure the Device Control message template on the **Message to user** tab.
7. You can add variables and links to the body of the message for the user by clicking the **Add variable** and **Add link** buttons. To add a variable to the template, place the cursor in the required place in the text, click the **Add variable** button, and select a variable in the drop-down list. To add a link to the template, place the cursor in the required place in the text and click the **Add link** button.

   If you want to restore the text of the message template, click the **Restore default** button.
8. Click **OK**.
9. Click the **Save** button to save the changes made.

How to change a message template in the Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the required devices belong.
2. In the workspace, select the **Policies** tab.
3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.

   You can also open the policy properties window by using the **Properties** item in the policy context menu or by clicking the **Configure policy settings** link located to the right of the list of policies in the section with the policy settings.
4. In the policy window, select **Security Controls** → **Device Control**.
5. In the **Message templates** section, click the **Configure** button.
6. This opens the **Message templates** window; in that window, configure the Device Control message template on the **Block message** tab.

You can add variables and links to the body of the message for the user by clicking the **Variable** and **Link** buttons. To add a variable to the template, place the cursor in the required place in the text, click the **Variable** button, and select a variable in the drop-down list. To add a link to the template, place the cursor in the required place in the text and click the **Link** button.

You can also restore the text of the message template by clicking the **Default** button.

7. Click **OK**.

8. Click **Apply**.

Granting temporary access to device

When configuring Device Control, the administrator may mistakenly block access to a device that the user needs for work. If the user believes that access to a device or an operation with device content was blocked by mistake, the user can request temporary access to the blocked device from the administrator of the corporate local network.

> The user can request temporary access if the administrator has the user allowed to do so. The administrator can configure this permission in the policy properties in the Web Console, in the Administration Console, or in the settings of the Device Control task.

Granting access to a blocked device involves the following steps:

1. The user creates an *access request file* and sends it to the administrator, for example, by email or in any available way (the administrator can configure this in the block message template). The user can request temporary access to the blocked device in the graphical interface of the application or on the command line.

2. The administrator creates an *access key* based on the access request file and passes it to the user, for example, by email or in any other way. Access to a blocked device is granted in the Web Console.

3. The user uploads the access key and gains temporary access to the blocked device. The user can upload the access key in the graphical user interface or on the command line of the application.

> Granting access to a blocked device is available only if Kaspersky Security Center 16.1 is deployed in the organization and the client device is able to establish a connection with the Administration Server.

How to create an access key for the blocked device in the Web Console

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. Select the administration group containing the relevant device and select the check box next to the name of the device.

3. Above the list of managed devices, click the **Grant access to the device in offline mode** button. If this button is not displayed above the list of devices, click the three dots button and select the **Grant access to the device in offline mode** command from the menu.

4. This opens the **Application Settings** window; in that window, in the **Device Control** section, click the **Browse** button and download the access request file received from the user.

   Information about the blocked device to which the user has requested access is displayed.

5. If necessary, change the duration in hours in the **Access duration** field.

   By default, **Access duration** is set to the value specified by the user when generating the access request file.

6. If necessary, change the value in the **Specify how long an access key can be used on the client device (in hours)** field.

   This field contains the time period during which the access key can be uploaded by the user.

7. Click the **Create key** button.

8. Save the access key file with the *.acode extension.

How to request and obtain temporary access on the command line

If the user believes that access to the device was blocked or an operation with the contents of the device was prohibited by mistake, the user can request temporary access to the blocked device from the administrator of the local network of the organization using the following Device Control management command:

```
Request temporary access to a blocked device

kesl-control --request-temporary-device-access --device-id <device identifier>  --access-duration <access
duration> --path <path to the access request file>
```

where:

`--device-id <device identifier>` is the ID of the blocked device to which you want to gain access.

`--access-duration <access duration>` is the period of time for which you want to gain access to the device (in hours). Possible values: 1 to 100

`--path <path to the access request file>` is the path to the directory in which you want to save the access request file with the .akey extension.

This command creates an access request file, which must be sent to the administrator, for example, by email or in any other way (the administrator can describe the preferred method in the template of the blocking message).

After receiving the access key from the administrator, you must enter the access key to gain temporary access to the device.

```
Upload an access key for a blocked device

kesl-control --upload-temporary-device-access-key --path <path to the file with the access key>
```

where:

`--path <path to the file with the access key>` is the path to the file with the device access key (file with the .acode extension).

This command outputs information about the granted access to the device and the access duration.

How to request and obtain temporary access in the graphical interface

When a device is connected, and access to that device is denied by Device Control, a window with a message about blocked access to the device is displayed.

You can request temporary access to a blocked device from your organization's local network administrator using the graphical interface:

- From the window with the message about blocked access to the device, by clicking **OK**
- From the main window of the application graphical interface

To request temporary access to a blocked device:

1. Open the main window of the application graphical interface.
2. In the lower part of the main window, click the **Temporary access** button.

   This opens the **Temporary access** window.

   You can also open the **Temporary access** window from the window with the message about blocked access to the device by clicking **OK**.
3. In the **Request access to the blocked device** section, in the list of connected devices, select the device to which you want to gain access.
4. In the **Device access duration (hours)** field, specify the time period for which you want to gain access to the device (in hours).
5. Click the **Create request access file** button.
6. In the opened window, specify the path to the directory in which you want to save the access request file with the .akey extension.
7. Send the access request file to the administrator, for example, by email or in any available way (the administrator can configure this in the block message template).

After getting the access key from the administrator, you can upload the access key to gain temporary access to the blocked device.

To get temporary access to a blocked device:

1. Open the main window of the application graphical interface.
2. In the lower part of the main window, click the **Temporary access** button.

   This opens the **Temporary access** window.
3. In the **Get access to the device** section, click the **Upload access key** button.
4. In the opened window, select the file with the device access key (file with the .acode extension) received from the administrator of the organization's local network.
5. A window is displayed with information about the device to which access has been granted and the access duration.
6. Click **OK**.

Web Control

Web Control manages user access to web resources. This allows you to reduce traffic consumption and reduce inappropriate use of work time. If a user tries to open a website to which access is restricted by Web Control, Kaspersky Endpoint Security blocks access or displays a warning.

Web Control allows restricting access to web resources by content category and data type, as well as blocking access to individual websites. You can restrict user access to, for example, the "Social networks" content category or other categories. The application determines the data type by the file format, not by extension.

How Web Control works

1. **The application checks requests to web resources**

   Web Control determines the content category and data type of a website using the following technologies:

   - Anti-virus databases.
   - Cloud services of Kaspersky Security Network.
   - The Heuristic analysis technology allows detecting threats that are not yet covered by Kaspersky databases.

2. **The application applies rules**

   The application applies Web Control rules in order of priority. The lower the priority number, the higher the priority of the rule. If multiple rules are applicable to a website, Web Control applies the rule with the highest priority.

   For example, the application may identify the corporate portal as a social network. To restrict access to social networks and provide access to the corporate web portal, create two rules: one block rule for the *Social networks* website category and one allow rule for the corporate web portal. The corporate web portal access rule must have a higher priority than the social network access rule.

3. **Completion of the scan**

   If a rule blocks access to a web resource, the application displays a block message in the browser. The resource is made unavailable.

   The user can send a request to the organization's administrator about the mistaken blocking if the user believes that the web page was blocked by mistake.

Configuring Web Control

1. **Configure Web Control rules**

   Web Control manages user access to websites by using *access rules*. These rules allow restricting access to websites for individual users, as well as configure an access schedule.

   For example, you can restrict access to websites in the *Internet communication* category for all users in the organization except for the IT department.

2. **Configure message templates**

Depending on the action of the access rule, Web Control displays a message to the user about visiting an unwanted website or a block message. When a website is blocked, the user can send a message to the administrator of the local network about the mistaken blocking.

Templates are provided for such messages.

> The templates cannot be edited on the command line.

3. **Enable Web Control**

   By default, Web Control is disabled. Enable the component in the Web Console or the Administration Console using the toggle switch, or on the command line using the following command:

```
kesl-control --start-task 26
```

Special considerations and limitations

- The application does not scan files inside archives. For example, if image files are archived, the application detects the data type as Archives rather than Image files.
- Kaspersky Endpoint Security monitors only HTTP and HTTPS traffic.
- When Web Threat Protection and Web Control are running simultaneously, the Web Threat Protection settings are applied to the web resource. This means a malicious or phishing website is blocked even if Web Control rules allow access to it.

How to create a rule of access to web resources

A *web resource access rule* is a set of filters and actions that Kaspersky Endpoint Security applies when users visit web resources. Access rules can include a rule schedule.

Rules restrict access to web resources by the following filters:

- **Content categories**. Web Control categorizes web resources by content and data type. This allows restricting user access to websites with a specific category of content (for example, *Payment systems*) and/or a specific data type (for example, *Executable files*).
- **Individual websites**. Web Control allows restricting user access to individual addresses or groups of addresses of web resources.

  Domains of web addresses are case-insensitive. If a rule contains a web address such as `examPLE.com`, Web Control will restrict access to `example.com`.

  If a filter by content category and a filter by individual websites are simultaneously configured in an access rule, Web Control does not restrict access to all websites of the specified content category, but only to the specified web addresses.

- **Filter by name of users and user groups**. Web Control allows restricting access to web resources for individual users or groups of users. For example, you can restrict access to social media websites for all users in the organization except for the IT department.

- **Rule schedule**. The rule schedule determines the time when the application controls access to the web resources specified in the rule. For example, you can restrict access to unwanted websites only during work hours.

If no blocking rules are created, HTTPS traffic is not decrypted.

How to create an access rule in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **Web Control**.
5. Make sure the toggle switch for the component is in the **Web Control ENABLED** position.
6. Under **Rules list**, select the default Web Control action:

   - **Allow all except the rules list**
   - **Block all except the rules list**
7. Click **Add**.

   This opens the form for adding a new access rule.
8. In the **Rule name** field, enter the rule name. The rule name must be unique.
9. In the **Priority** field, set the access rule priority.
10. Select the action that you want Web Control to apply to web resources when the rule is triggered:

    - **Allow**. Web Control allows the user to access the web resource.
    - **Block**. Web Control blocks the user's access to the web resource and displays a message that access is blocked. By clicking the links in the blocking message, the user can send a message to the local network administrator to report the blocking mistake.
    - **Inform**. Web Control displays a warning about visiting an unwanted web resource. If the user believes the warning is incorrect, the link in the warning allows the user to go to a web page or send a request to the local network administrator of the organization.

11. Select an access rule filter:

    - **Content categories**. Specify the content categories that you want the access rule to control. You can select multiple categories.

    - **Individual websites**. Specify a website address or group of websites.

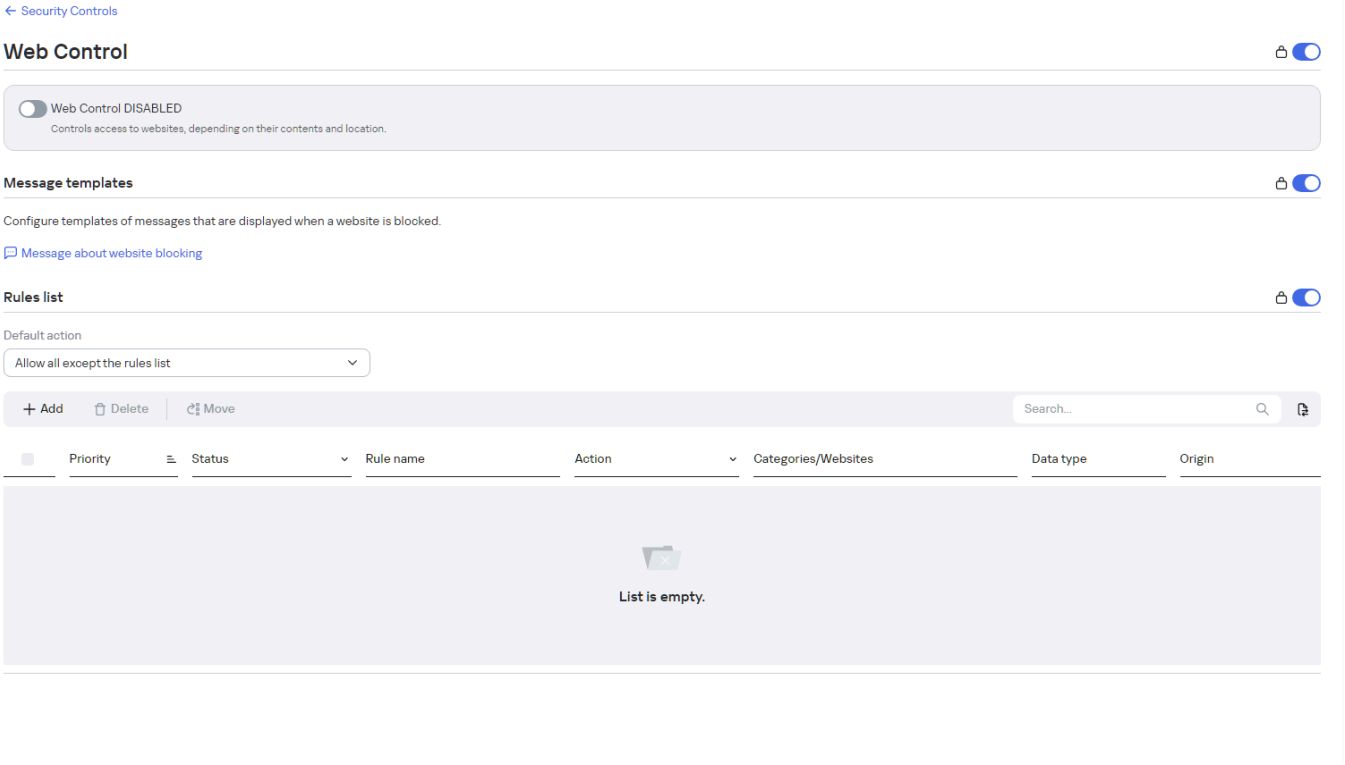
    > In the Web Console, you cannot set up a filter by content category and by individual websites simultaneously.

12. If necessary, specify the data types that you want to be filtered by the application.

13. Select the users or user group to which the access rule will apply. By default, the rule applies to all users.

14. If necessary, set an access schedule. By default, the rule is always applied.

15. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Web Control

How to create an access rule on the command line

1. Make sure that the Web Control component is enabled:

   ```
   kesl-control --get-settings 26
   ```

   The component must have the **Started** status.

2. If the component is disabled, run the command:

   ```
   kesl-control --start-task 26
   ```

3. select the default Web Control action:

```
kesl-control --set-settings 26 WebControlDefaultAction=<Allow|Block>
```

4. Add a new access rule with ID `#`:

   a. Enable the rule:

   ```
   kesl-control --set-settings 26 Rules.item_#.Enabled=Yes
   ```

   b. Enter the rule name:

   ```
   kesl-control --set-settings 26 Rules.item_#.Name=<rule name>
   ```

   c. Specify the action that you want Web Control to apply to web resources when the rule is triggered:

   ```
   kesl-control --set-settings 26 Rules.item_#.WebControlAction=<Allow|Block|Notify>
   ```

   d. If you need to filter web resources by content category:

   ```
   kesl-control --set-settings 26 Rules.item_#.UseCategories=<ContentOnly|FormatOnly|ContentAndFormat>
   kesl-control --set-settings 26 Rules.item_#.ContentCategories.item_#.ContentCategory=<category>
   [Rules.item_#.FormatCategories.item_#.FormatCategory=<format>]
   ```

   e. If you need to filter individual web resources:

   ```
   kesl-control --set-settings 26 Rules.item_#.UseUrls=Yes
   kesl-control --set-settings 26 Rules.item_#.Urls.item_#=<web address>
   ```

   f. If necessary, specify the users to which the rule will apply:

   ```
   kesl-control --set-settings 26 Rules.item_#.UsePrincipals=Yes
   kesl-control --set-settings 26 Rules.item_#.Principals.item_#.Name=<user name|@group name>
   ```

   g. If necessary, specify a schedule for the rule:

   ```
   kesl-control --set-settings 26 Rules.item_#.Schedules.item_#.Id=<ID> Rules.item_#.Schedules.item_#.Name=
   <schedule name> Rules.item_#.Schedules.item_#.DaysHours=<day of the week|hour>
   ```

5. To view the list of Web Control rules, run the following command:

```
kesl-control --get-settings 26
```

Symbols

Setting	Description
`WebControlDefaultAction`	The action that Web Control applies to web resources that are not specified in any access rules.
`Enabled=Yes`	Enable the access rule with ID `#`.
`Name`	Name of the rule. The rule name must be unique.
`WebControlAction`	The action that Web Control applies to web resources when the rule is triggered: `Allow` (default value) – allow access to the web resource. `Block` – block access to the web resource. `Notify` – display a warning about visiting an unwanted web resource. By clicking links in the warning message, the user can access the requested web resource.
`UseCategories`	Use of filters by content categories and data type categories in the rule: `None` (default) – do not use a web resource content filter. `ContentOnly` – use the content category filter in the rule. `FormatOnly` – use the data type category filter in the rule. `ContentAndFormat` – use the content category filter and the data type category filter in the rule.
`ContentCategories.item_#.ContentCategory`	Content categories.
`FormatCategories.item_#.FormatCategory`	Data type category: `Video` – Video files `Audio` – Audio files `OfficeDocument` – Office application files `Executable` – Executable files `Archives` – Archives `Images` – Image files `Scripts` – Scripts
`UseUrls=Yes`	Use of individual websites in a filter rule.
`Urls.item_#`	The address of the web resource for which the rule controls access. You can use masks to specify the web resource address.
`UsePrincipals=Yes`	Use of a filter of users that are covered by the web resource access rule.
`Principals.item_#.Name`	The user or group of users that is covered by the web resource access rule: `<user name>` is the name of the user to which the rule applies. `@<group name>` is the name of the group of users to which the rule applies.
`Schedules.item_#.Id`	Schedule ID.
`Schedules.item_#.Name`	Specifies a schedule name.
`Schedules.item_#.DaysHours`	Specifies time intervals for a schedule: `<day of week>` is the day of the week. You can use either the full week day names or abbreviations (for example, for Monday, you can specify `Mo`, or `Mon`, or `Monday`). For week days, you can specify intervals or specific days. The week starts from Sunday. `<hour>` – Hours [0:24]. You can specify only intervals for hours.

How to modify Web Control message templates

Depending on the action specified in the access rule, when a user attempts to access web resources, Web Control displays a message to the user (by replacing the HTTP server response with an HTML page containing a message):

- **Warning.** The message displayed to the user when trying to visit an unwanted resource. The application displays this message if the **Inform** action is selected for the rule.

  If the user believes the warning is incorrect, the link in the warning allows the user to go to a web page or send a request to the local network administrator of the organization.

- **Blocked web resource message** The message that is displayed to the user when an unwanted web resource is blocked. The application displays this message if the **Block** action is selected for the rule.

  If a user believes that a web resource has been blocked by mistake, the link in the web resource blocking message allows the user to submit a request to the local network administrator of the organization.

Templates are provided for warning messages, messages about blocking a web resource, and requests to the local network administrator of the organization. Special variables are provided for managing the message templates (for example, `%USER_NAME%`). Variables allow a single message template to be used for different computers. When generating a message, Kaspersky Endpoint Security retrieves the value of the variable from the operating system settings and inserts it into the message matching the specific computer, user, and event.

The templates cannot be edited on the command line.

How to edit the message template in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **Web Control**.
5. Under **Message templates**, click the **Message about website blocking** link.

   This opens the window with message templates.
6. Configure the Web Control message templates:

   - **Warning**. The template of the warning displayed to the user when trying to visit an unwanted resource.
   - **Message about blocking**. The template of the message displayed when an unwanted web page or website is blocked.
   - **Message to administrator**. Template of a message to the administrator. Used if the user believes the web page has been blocked by mistake. After the user requests access, the application sends a *Web page access blockage message to administrator* event to Kaspersky Security Center. The event description contains the message to the administrator with the variables replaced by their values. If no Kaspersky Security Center solution is deployed in your organization or there is no connection with the Administration Server, the application will send a message to the administrator's specified email address.

   If you want to restore the text of the message template, click the **Reset to default text** button.
7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to change a message template in the Administration Console

1. In the **Managed devices** folder in the Administration Console tree, open the folder with the name of the administration group to which the required devices belong.
2. In the workspace, select the **Policies** tab.

3. In the list of policies, select the required policy and open the **Properties: <Policy name>** window.

   You can also open the policy properties window by using the **Properties** item in the policy context menu or by clicking the **Configure policy settings** link located to the right of the list of policies in the section with the policy settings.

4. In the policy window, select **Security Controls** → **Web Control**.

5. In the **Message templates** section, click the **Configure** button.

6. This opens the **Message templates** window; in that window, configure the Web Control message templates on the following tabs:

   - **Warning**. The input field contains the template for the message that appears when a rule is triggered that warns about an attempt to access an undesirable web resource.

   - **Block message**. The entry field contains the template of the message that appears if a rule that blocks access to a web resource is triggered.

   - **Complaint to administrator**. The input field contains the template for a complaint to be sent to the administrator of the corporate LAN when the user believes that a blocked web resource should not be blocked. After a user requests access, Kaspersky Endpoint Security sends a *Message to the administrator about denied access to a web page* event to Kaspersky Security Center. The event description contains the message to the administrator with the variables replaced by their values. You can view these events in the Kaspersky Security Center Administration Console using the **User requests** selection. If no Kaspersky Security Center solution is deployed in your organization or there is no connection with the Administration Server, the application will send a message to the administrator's specified email address.

   On the **Warning** and **Block message** tabs, you can add variables and links to the messages for the user by using the **Variable** and **Link** buttons.

   You can restore the text of the message template by clicking the **Default** button.

7. Click **OK**.

8. Click **Apply**.

Rules for creating web resource address masks

A *web resource address mask* ("address mask") can be convenient when a lot of similar addresses of web resources must be entered when creating a web resource access rule. One skillfully-formed address mask can replace a large number of addresses of web resources.

When creating an address mask, the following rules apply:

1. The `*` character replaces any sequence of zero or more characters.

   For example, if you enter the address mask `*abc*`, the web resource access rule applies to all addresses containing the sequence `abc`. Example: `http://www.example.com/page_0-9abcdef.html`.

2. The character sequence `*.` lets you select all domains of an address, i.e. it represents a *domain mask*. The domain mask `*.` is interpreted as any domain name, subdomain name, or an empty string.

Example: the following addresses match the `*.example.com` mask:

- `http://pictures.example.com` – the domain mask `*.` matches `pictures.`.
- `http://user.pictures.example.com` – the domain mask `*.` matches `pictures.` and `user.`.
- `http://example.com` – the domain mask `*.` is interpreted as an empty string.

3. The character sequence `www.` at the beginning of an address mask is interpreted as the sequence `*.`.

   Example: The address mask `www.example.com` is interpreted as `*.example.com`. The mask matches the addresses `www2.example.com` and `www.pictures.example.com`.

4. If an address mask does not begin with a `*` character, the address mask matches the same content that it would match if it started with `*.`.

5. If an address mask ends with a character other than `/` or `*`, the address mask matches the same content that it would match if it ended with `/*`.

   Example: the address mask `http://www.example.com` matches addresses of the form `http://www.example.com/abc`, where `a`, `b`, `c` are any characters.

6. If an address mask ends with a `/` character, the address mask matches the same content that it would match if it ended with `/*`.

7. The character sequence `/*` at the end of an address mask is interpreted as `/*` or an empty string.

8. When web resource addresses are compared to an address mask, the protocol (http: or https:) is taken into consideration.

   - If there is no network protocol in the address mask, the address mask matches addresses with any network protocol.

     Example: The address mask `example.com` matches the addresses `http://example.com` and `https://example.com`.

   - If a network protocol is present in an address mask, only addresses with the same network protocol will match the address mask.

     Example: the address mask `http://*.example.com` matches the address `http://www.example.com` but does not match the address `https://www.example.com`.

9. An address mask enclosed in double quotes is interpreted without any further substitutions, except for the `*` character if it was initially included in the address mask. For address masks enclosed in double quotes, rules 5 and 7 are not enforced (see examples 14–18 in the table below).

10. The evaluation of a web resource address mask does not consider the user name and password, connection port, or case.

Examples of applying rules to build address masks

No.	Address mask	Web resource address	Does the address match the address mask?	Comment
1	*.example.com	http://www.123example.com	No	See rule 1.
2	*.example.com	http://www.123.example.com	Yes	See rule 2.
3	*example.com	http://www.123example.com	Yes	See rule 1.

No.	Address mask	Web resource address	Does the address match the address mask?	Comment
4	*example.com	http://www.123.example.com	Yes	See rule 1.
5	http://www.*.example.com	http://www.123example.com	No	See rule 1.
6	www.example.com	http://www.example.com	Yes	See rules 3, 2, and 1.
7	www.example.com	https://www.example.com	Yes	See rules 3, 2, and 1.
8	http://www.*.example.com	http://123.example.com	Yes	See rules 3, 4, and 1.
9	www.example.com	http://www.example.com/abc	Yes	See rules 3, 5, and 1.
10	example.com	http://www.example.com	Yes	See rules 3 and 1.
11	http://example.com/	http://example.com/abc	Yes	See rule 6.
12	http://example.com/*	http://example.com	Yes	See rule 7.
13	http://example.com	https://example.com	No	See rule 8.
14	"example.com"	http://www.example.com	No	See rule 9.
15	"http://www.example.com"	http://www.example.com/abc	No	See rule 9.
16	"*.example.com"	http://www.example.com	Yes	See rules 1 and 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Yes	See rules 1 and 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Yes	See rules 9 and 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	An address mask contains more information than a web resource address.

Application Control

Application Control manages the launch of third-party applications on user devices. This reduces the risk of malware infection on the protected device.

To use the component, a license that includes the corresponding function is required.

How Application Control works

1. **User attempts to run a third-party application**

2. **Application Control applies rules**

   Application Control sequentially applies rules to the application being launched. Depending on the selected rule mode, the component *controls* applications being launched or *tests* rules. The priority of a block rule is higher than the priority of an allow rule.

3. **Completion of the scan**

   If the rules prevent the execution of the application, the component blocks the launch of this application and generates an *Application startup prohibited* event. In testing mode, the component does not block the launch of this application and generates the *Application startup prohibited in test mode* event.

Configuring Application Control

1. **Take an inventory of applications**

   Use the Inventory task to get a list of applications installed on the protected devices. Based on this information, create a list of applications that you want to prevent from running.

2. **Select the Application Control operating mode**

   The Application Control component can operate in one of two modes:

   - *Allow all except the rules list*. Application Control allows users to run any third-party applications, except those that are prohibited by the rules.
   - *Block all except the rules list*. Application Control allows users to run any third-party applications, except those that are allowed and not prohibited by the rules.

   The choice of Application Control mode depends on the security policy of your organization, as well as how many applications you want to control.

3. **Create application categories**

   Define the categories of allowed or denied applications. Application categories are intended for all devices in the corporate network, regardless of administration groups. Application categories let you configure rules for a group of applications rather than based on inclusion and exclusion conditions.

   It is recommended to create a "Work applications" category that covers the standard set of applications that are used at the company. If different user groups use different sets of applications in their work, a separate application category can be created for each user group.

   > We recommend configuring application categories in Kaspersky Security Center.

4. **Configure Application Control rules**

   The component controls the launch of applications based on *application control rules*, which define conditions under which Application Control allows or denies the launch of a third-party application for a selected group of users.

5. **Test Application Control rules**

   Application Control is disabled by default. We recommend enabling Application Control in testing mode and testing the created application control rules. The application will not block third-party applications from running, but will send notifications about their launch to the Administration Server.

6. **Learn how the Application Control rules work**

   Review the report about the operation of Application Control in testing mode. After reviewing the information, adjust your Application Control rules as necessary.

7. **Enable the use of Application Control rules**

   In this mode, Kaspersky Endpoint Security prevents the execution of third-party applications if the rules do not allow running these applications.

How to enable the use of Application Control rules in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **App Control**.
5. Make sure the toggle switch for the component is in the **App Control ENABLED** position.
6. Under **Action on starting applications**, select the **Apply rules** action for Application Control.
7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to enable the use of Application Control rules on the command line

To select the test mode for Application Control, run the following command:

```
kesl-control --set-settings 21 AppControlRulesAction=ApplyRules
```

The Kaspersky Security Center administrator or a local user with the admin role assigned in the application can allow or deny process start under the root account using the Application Control.

Special considerations and limitations

- Application Control does not control the launch of Snap, Flatpak, or AppImage applications.
- The Application Control task does not control the launching of scripts from interpreters that are not supported by Kaspersky Endpoint Security, or the launching of scripts that are not passed to the interpreter via the command line. Kaspersky Endpoint Security supports the following interpreters: python, perl, bash, ssh.
- If the rules allow the interpreter to run, Application Control does not block a script launched from that interpreter. If the launch of at least one script specified in the interpreter command line is prohibited by the rules, Kaspersky Endpoint Security blocks all the scripts specified in the interpreter command line. Exclusion: cat script.py | python.

Application inventory

To create optimal Application Control rules, it is recommended to first get a picture of the applications that are used on protected devices on the corporate LAN. The *Inventory* task lets you get the following information:

- The name and version of the third-party application
- A short description

To use the task, a license that includes the corresponding function is required.

The Kaspersky Security Center database can store information about up to 150,000 processed files. Once the limit is reached, new files will not be processed. To resume the inventory, you need to delete from the protected device the files that had been added to the Kaspersky Security Center database during the previous inventory.

Configuring and running the Inventory task

1. **Create an Inventory task**

   How to create an Inventory task in the Web Console

   1. In the main window of the Web Console, select **Tasks**.

      The list of tasks opens.

   2. Click **Add**.

      The Task Wizard starts.

   3. Configure the task settings:

      a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux 12.5**.

      b. In the **Task type** drop-down list, select **Inventory**.

      c. In the **Task name** field, enter the task name.

      d. In the **Devices to which the task will be assigned** block, select the task scope.

   4. Select devices according to the selected task scope option.

   5. Finish the wizard.

   How to create an Inventory task on the command line

To create a task, run the following command:

```
kesl-control --create-task <task name> --type InventoryScan
```

where `<task name>` is the name of the new task.

This command returns the ID of the created task.

Example of the command execution result:

Task created (task ID: 100)

2. **Configure inventory scopes**

At least one inventory scope must be specified for the task to start. By default, the *Executable commands – /usr/bin* scope is set.

Kaspersky Endpoint Security scans objects in the specified scopes, in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

How to configure an inventory scope in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the created Inventory task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Go to the **Inventory scopes** section.

5. Click **Add**.

   This opens the window for adding inventory scopes.

6. In the **Scope name** field, enter a name for the inventory scope, for example, *Files on the desktop*.

7. In the **Path** field, specify the path to an individual file or directory, for example, `/path/to/folder`. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

8. If necessary, specify masks for object names in the command shell format, for example, `*.txt`, `file?.*`. Add masks one at a time.

9. Save your changes.

How to configure an inventory scope on the command line

1. Run the following command:

```
kesl-control --set-settings <task name | task ID> ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. To check the current settings, run the following command:

```
kesl-control --get-settings <task name | task ID>
```

Symbols

Inventory task settings

Setting	Description
`UseScanArea=Yes`	Enabling an inventory scope with an `#` ID. You can temporarily disable an inventory scope scan instead of deleting the scope. To do this, set `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description of the inventory scope. The maximum length of the string specified using this setting is 4096 characters.
`AreaMask.item_#`	Inventory scan scope limitation. In the inventory scope, the application scans only the objects that are specified using the masks in the shell format. You can specify several `ScanScope.item_#.AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order. For example, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Path to the directory with objects to be scanned. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask. Default value: `/usr/bin`

3. **If necessary, edit the task settings**

How to configure the Inventory task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the created Inventory task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Go to the **Inventory settings** section.

5. Select an action with the "Golden Image" category of applications:

   - **No changes** – do not change the Golden Image category after completing the inventory. This is the default selection. This option is used when you want to get a list of third-party applications used on the device, but not to add them to the "Golden Image" category.

   - **Update or create (if does not exist)** – adds applications detected on the device by the inventory task to the "Golden Image" category. If the category does not exist, it is created. If the category exists, the list of applications in the category is updated.

   - **Remove** – clear the Golden Image application category. The category is cleared immediately the task is started, without doing an inventory of files on the device.

6. If necessary, select the following check boxes:

   - **Script files inventory**. Check for scripts in the inventory scope. The application sends this information to Kaspersky Security Center.
   - **Scan all executables**.
   - **Scan binaries**. Scanning binary files (files with the extensions .elf, .java and .pyc).

7. Save your changes.

How to configure the Inventory task on the command line

Execute the command:

```
kesl-control --set-settings <task name | task ID> ScanScripts=<Yes|No> ScanBinaries=<Yes|No>
ScanAllExecutable=<Yes|No> GoldenImageAction=<DoNothing|Create|Remove>
```

Symbols

Inventory task settings

Setting	Description
`ScanScripts`	Check for scripts in the inventory area: `Yes` (default value) — Scan scripts. `No` — Do not scan scripts.
`ScanBinaries`	Scanning binary files (files with the extensions .elf, .java and .pyc): `Yes` (default value) — Scan binaries. `No` — Do not scan binaries.
`ScanAllExecutable`	Scanning executable files: `Yes` (default value) — Scan files with an executable bit. `No` — Do not scan files with an executable bit.
`GoldenImageAction`	The action that Kaspersky Endpoint Security must perform with the Golden Image application category upon completion of the Inventory task: `DoNothing` (default) – do not change the Golden Image application category. `Create` – add detected applications to the "Golden Image" application category. If the category does not exist, it is created. If the category exists, the list of applications in the category is updated. `Remove` – clear the Golden Image application category. The category is cleared immediately the task is started, without doing an inventory of files on the device.

4 Configure exclusion scopes

An exclusion has a higher priority than an inventory scope. An excluded object is not scanned even if it is in an inventory scope. If the inventory scope is defined on a lower level than the excluded directory, the application skips this inventory scope while running the task.

How to configure an exclusion scope in the Web Console

1. In the main window of the Web Console, select **Tasks**.
2. The list of tasks opens.
3. Click the created Inventory task.

   The task properties window opens.
4. Select the **Application settings** tab.

5. Go to the **Exclusion scopes** section.

6. Click **Add**.

   This opens the window for adding exclusion scopes.

7. In the **Scope name** field, specify the name of the exclusion scope, for example, *System files*.

8. In the **Path** field, specify the path to an individual file or directory (for example, `/path/to/folder`). Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

9. Specify masks of object names in the command shell format (for example, `*.txt` or `file?.*`). Add masks one at a time.

10. Save your changes.

How to configure an exclusion scope on the command line

1. Run the following command:

```
kesl-control --set-settings <task name | task ID>       ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. To check the current settings, run the following command:

```
kesl-control --get-settings <task name | task ID>
```

Symbols

Inventory task settings

Setting	Description
`UseScanArea`	Excludes the specified scope from the inventory. You can temporarily disable an exclusion scope instead of deleting the scope. To do this, set `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description of the inventory exclusion scope.
`AreaMask.item_#`	Limitation of the exclusion scope. In the exclusion scope, the application excludes from scans only the objects specified using masks in the shell format. You can specify several `ExcludedFromScanScope.item_#.AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order. For example, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	The path to the directory to be excluded from inventory. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

Example of excluding the `/tmp` directory from the inventory:

```
kesl-control --set-settings 100 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 Run the task

How to run the Inventory task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Select the check box next to the created task.

3. Click **Start**.

How to tun an Inventory task on the command line

To run the task, run the following command:

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `[-W]` enables the output of current events related to this task.
- `[--progress]` enables the display of task progress.

Viewing a list of detected applications

To view the list of applications detected on the devices in the Web Console:

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the created Inventory task.

   The task properties window opens.

3. Select the **Results** tab.

```
View the list of applications detected on the client device
kesl-control --get-app-list [--json]
```

Kaspersky Endpoint Security displays the following information about the detected applications:

- Date and time of the inventory
- Number of applications
- The list of applications containing the following information:
  - Path to the application.
  - Application hash sum.

- Application type. For example, `Script`, `Executable`.
- Categories that the application belongs to (if they were previously created). You can view the list of created application categories using the following command:

  ```
  kesl-control --get-categories
  ```

> When you add a new category, its information is not automatically updated in the application list. To update the list of applications, you must run the Inventory task again.

How to configure the Application Control operating mode

The Application Control component can operate in one of two modes:

- *Allow all except the rules list*. Application Control allows users to run any third-party applications, except those that are prohibited by the rules.
- *Block all except the rules list*. Application Control allows users to run any third-party applications, except those that are allowed and not prohibited by the rules.

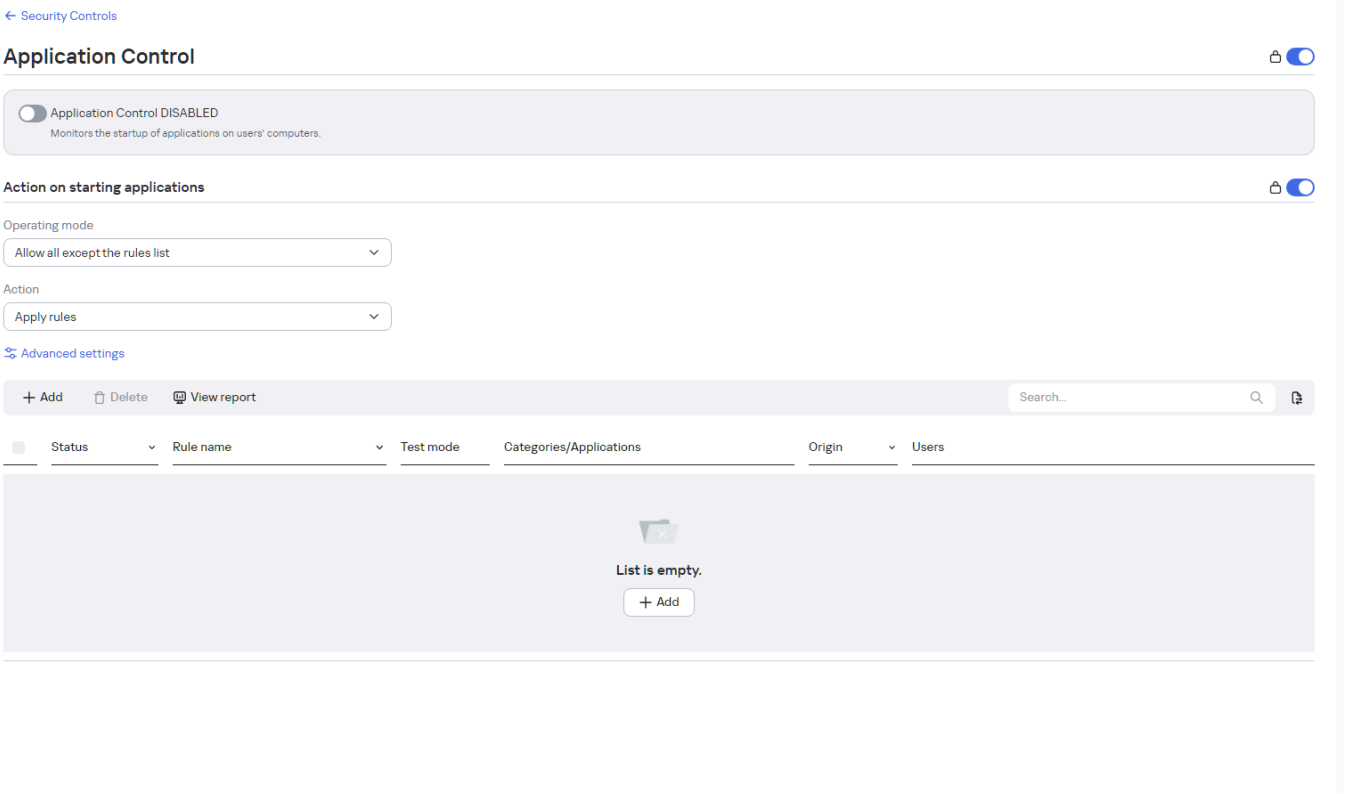
The choice of Application Control mode depends on the security policy of your organization, as well as how many applications you want to control.

How to configure the Application Control operating mode in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **App Control**.
5. Make sure the toggle switch for the component is in the **App Control ENABLED** position.
6. Under **Action on starting applications**, select the Application Control operating mode:
   - **Allow all except the rules list**
   - **Block all except the rules list**

7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Application Control

How to configure the Application Control operating mode on the command line

Execute the command:

```
kesl-control --set-settings 21 AppControlMode=<AllowList|DenyList>
```

Symbols

Command options

Setting	Description
`AppControlMode`	`AllowList` – Kaspersky Endpoint Security prevents users from launching any applications that are not specified in the Application Control rules. `DenyList` (default value) – Kaspersky Endpoint Security allows users to launch any applications that are not specified in the Application Control rules.

Creating application categories

For more convenience when creating Application Control rules, you can create *application categories*.

Kaspersky Endpoint Security determines the category of an application using the following technologies:

- Anti-virus databases.
- Cloud services of Kaspersky Security Network.
- The Heuristic analysis technology allows detecting threats that are not yet covered by Kaspersky databases.

In Kaspersky Endpoint Security for Linux, categories can be created based on the following parameters:

- Name of the application's executable file.
- Name of the directory with the application's executable file.
- Hash of the application's executable file. Only SHA256 can be used.

  You can use masks to specify the names of files and directories.

  Rules for specifying masks

  You can use the * character (any sequence of characters) or the ? character (any one character) as the file or directory name mask.

  You can put the * character to represent any set of characters (including an empty set) in a file or directory name that includes the / character. For example, `/dir/*/file*/` or `/dir/file*/`.

  You can put a single ? character to represent any one character (including `/`) in the file or directory name.

It is recommended to create a "Work applications" category that covers the standard set of applications that are used at the company. If different user groups use different sets of applications in their work, a separate application category can be created for each user group.

Kaspersky Endpoint Security for Linux does not support KL categories.

To create an application category in Kaspersky Security Center:

1. In the main window of the Web Console, select **Asset management** → **Third-party applications** → **Application categories**.
2. Click **Add**.

   The user category creation wizard starts.
3. Follow the instructions of the user category creation wizard.

Step 1.

At this step, specify the name of the application category and select one of the following application category types:

- *Category with content added manually. Data of executable files is manually added to the category*. If you selected this type of category, in the *Conditions* and *Exclusions* steps you will be able to define the criteria whereby executable files will be included into the category.
- *Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category*. If you selected this type of category, at the next step you will be able to specify a folder from which executable files will be automatically included in the category.
- *Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category*. If you selected this type of category, on the next step you will be able to specify a computer whose executable files will be automatically included in the category.

Step 2.

This step is available if you selected the following category type: **Category with content added manually. Data of executable files is manually added to the category**.

At this step, select criteria for inclusion of applications in the category:

- **From KL category**

  If this option is selected, you can specify a Kaspersky application category as the condition for adding applications to the custom category. A *KL category* is a list of applications that have shared theme attributes. The list is maintained by Kaspersky experts. For example, the KL category known as "Office applications" includes applications from the Microsoft Office suite, Adobe Acrobat, and others.

  You can select all KL categories to generate an extended list of trusted applications.

- **Select certificate from repository**

  If this option is selected, you can specify certificates from the store. The category condition matches only executable files that are signed with the specified certificate.

  If you have selected a certificate as a rule-triggering condition, ensure that this certificate is added to the trusted system storage on the computer, and check the trusted system storage usage settings in the application.

- **Specify path to application (masks supported)**

  If this option is selected, you can specify a file or folder on the client device, from which executable files will be added to the custom application category. You can use regular expressions, such as `C:\path_to_exe\*`, for example: `C:\Program Files\Internet Explorer\*`.

- **Removable drive**

  If this option is selected, you can specify the type of media (any or removable drive) from which the application is being started. Application started from media of the selected type are added to the custom application category.

- **Hash, metadata, or certificate**:

  - **Select from the list of executable files**

    If this option is selected, you can select applications to be added to the category from the list of executable files on the client device.

  - **Select from the application registry**

    If this option is selected, the registry of applications is displayed. After you select an application from the registry, a window is opened with settings pre-filled with metadata from the selected application:

    - File name

    - File version You can specify an exact version or enter a condition, for example, "greater than 5.0".

- Application name.
- Application version. You can specify an exact version or enter a condition, for example, "greater than 5.0".
- Vendor.

Note that only executable files that match the specified parameters are blocked, but not the launch of the selected application as such. If the selected metadata match the metadata of the executable file that is started when you start the application, you can proceed to the next step. Otherwise, you need to edit the values manually to make them match the metadata of the executable file.

- **Set manually**

  If this option is selected, you need to specify a file hash, metadata, or certificate as the condition for adding applications to a custom category.

  File Hash

  Depending on the version of the security application installed on devices in your network, you need to select a hashing algorithm that Kaspersky Endpoint Security applies to files in the category. Information about hash values calculated by hash functions is stored in the database of the Administration Server.

  SHA256 is a cryptographic hash function whose algorithm has no known weaknesses; it is currently considered the most secure hash function. Kaspersky Endpoint Security 10 and later supports SHA256. The MD5 hash function is supported for Kaspersky Endpoint Security versions earlier than 10.

  Select one of the hash function that you want Kaspersky Endpoint Security to apply to files in the category:

  - If all instances of security applications installed in your network are Kaspersky Endpoint Security versions 10 or later, select the **SHA256** check box. We do not recommend creating a category based on the SHA256 hash of the executable file for Kaspersky Endpoint Security 10 or earlier. This can cause the security application to malfunction. In this case, you can use the MD5 cryptographic hash function for files of the category.
  - If you have earlier versions than Kaspersky Endpoint Security 10 installed in your network, select the **MD5 hash** check box. Adding a category based on the MD5 hash of the executable file for Kaspersky Endpoint Security 10 or later is not possible. In this case, you can use the SHA256 cryptographic hash function for files of the category.
  - If your network includes devices that use Kaspersky Endpoint Security versions earlier as well as later than 10, select both the **SHA256** check box and the **MD5 hash** check box.

  Metadata

  If this option is selected, you can specify file metadata such as file name, file version, and vendor. A category condition matches only executable files with identical metadata.

  Certificate

  If this option is selected, you can specify certificates from the store. The category condition matches only executable files that are signed with the specified certificate.

- **From MSI package/archive folder**

  If this option is selected, you can specify an MSI installer file as the condition for adding applications to the custom category. Metadata of the application installer are sent to the Administration Server. Applications whose installer metadata match the specified MSI installer are added to the custom application category.

Step 3.

This step is available if you selected the following category type: **Category with content added manually. Data of executable files is manually added to the category**.

Applications specified at this step are excluded from the category even if these applications were specified at the "Configuring the conditions for including applications in a category" step.

At this step, select criteria for exclusion of applications from the category:

- **From KL category**

  If this option is selected, you can specify a Kaspersky application category as the condition for adding applications to the custom category. A *KL category* is a list of applications that have shared theme attributes. The list is maintained by Kaspersky experts. For example, the KL category known as "Office applications" includes applications from the Microsoft Office suite, Adobe Acrobat, and others.

  You can select all KL categories to generate an extended list of trusted applications.

- **Select certificate from repository**

  If this option is selected, you can specify certificates from the store. The category condition matches only executable files that are signed with the specified certificate.

  If you have selected a certificate as a rule-triggering condition, ensure that this certificate is added to the trusted system storage on the computer, and check the trusted system storage usage settings in the application.

- **Specify path to application (masks supported)**

  If this option is selected, you can specify a file or folder on the client device, from which executable files will be added to the custom application category. You can use regular expressions, such as `C:\path_to_exe\*`, for example: `C:\Program Files\Internet Explorer\*`.

- **Removable drive**

  If this option is selected, you can specify the type of media (any or removable drive) from which the application is being started. Application started from media of the selected type are added to the custom application category.

- **Hash, metadata, or certificate**:

  - **Select from the list of executable files**

    If this option is selected, you can select applications to be added to the category from the list of executable files on the client device.

- **Select from the application registry**

  If this option is selected, the registry of applications is displayed. After you select an application from the registry, a window is opened with settings pre-filled with metadata from the selected application:

  - File name
  - File version You can specify an exact version or enter a condition, for example, "greater than 5.0".
  - Application name.
  - Application version. You can specify an exact version or enter a condition, for example, "greater than 5.0".
  - Vendor.

  Note that only executable files that match the specified parameters are blocked, but not the launch of the selected application as such. If the selected metadata match the metadata of the executable file that is started when you start the application, you can proceed to the next step. Otherwise, you need to edit the values manually to make them match the metadata of the executable file.

- **Set manually**

  If this option is selected, you need to specify a file hash, metadata, or certificate as the condition for adding applications to a custom category.

  File Hash

  Depending on the version of the security application installed on devices in your network, you need to select a hashing algorithm that Kaspersky Endpoint Security applies to files in the category. Information about hash values calculated by hash functions is stored in the database of the Administration Server.

  SHA256 is a cryptographic hash function whose algorithm has no known weaknesses; it is currently considered the most secure hash function. Kaspersky Endpoint Security 10 and later supports SHA256. The MD5 hash function is supported for Kaspersky Endpoint Security versions earlier than 10.

  Select one of the hash function that you want Kaspersky Endpoint Security to apply to files in the category:

  - If all instances of security applications installed in your network are Kaspersky Endpoint Security versions 10 or later, select the **SHA256** check box. We do not recommend creating a category based on the SHA256 hash of the executable file for Kaspersky Endpoint Security 10 or earlier. This can cause the security application to malfunction. In this case, you can use the MD5 cryptographic hash function for files of the category.
  - If you have earlier versions than Kaspersky Endpoint Security 10 installed in your network, select the **MD5 hash** check box. Adding a category based on the MD5 hash of the executable file for Kaspersky Endpoint Security 10 or later is not possible. In this case, you can use the SHA256 cryptographic hash function for files of the category.
  - If your network includes devices that use Kaspersky Endpoint Security versions earlier as well as later than 10, select both the **SHA256** check box and the **MD5 hash** check box.

  Metadata

  If this option is selected, you can specify file metadata such as file name, file version, and vendor. A category condition matches only executable files with identical metadata.

  Certificate

If this option is selected, you can specify certificates from the store. The category condition matches only executable files that are signed with the specified certificate.

- **From MSI package/archive folder**

  If this option is selected, you can specify an MSI installer file as the condition for adding applications to the custom category. Metadata of the application installer are sent to the Administration Server. Applications whose installer metadata match the specified MSI installer are added to the custom application category.

Step 4. Settings

This step is available if you selected the following category type: **Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category**.

At this step, click the **Add** button and specify the computers whose executable files will be added to the application category by Kaspersky Security Center.

At this step, configure the following settings:

- **Algorithm for hash function calculation**

  Depending on the version of the security application installed on devices in your network, you need to select a hashing algorithm that Kaspersky Security Center applies to files in the category. Information about hash values calculated by hash functions is stored in the database of the Administration Server.

  SHA256 is a cryptographic hash function whose algorithm has no known weaknesses; it is currently considered the most secure hash function. Kaspersky Endpoint Security for Linux supports SHA256.

  Select one of the hashing algorithm to apply to files in the category:

  - If you are using Kaspersky Endpoint Security for Linux on the protected devices, select the **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)** check box.

  - If you are using Kaspersky Endpoint Security for Windows on the protected devices, select the **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** check box.

  If you are using the applications both for Windows and Linux on your network, select both check boxes.

- **Synchronize data with Administration Server storage**

  Select this option if you want the Administration Server to periodically check the specified folder (or folders) for changes.

  This setting is disabled by default.

  If you enable this parameter, specify the period in hours for checking the specified folder (or folders) for changes. By default, the period is set to 24 hours.

- **File type**

  In this section, you can specify the file type that you want to use to create the application category.

  All files. The category will match all files. This option is enabled by default.

  Only files outside the application categories. The category will match only files outside application categories.

- **Folders**

  In this section, you can specify folders of selected computers that contain files that you want to use to create the application category.

  All folders. The category will match all folders. This option is enabled by default.

  Specified folder. The category will match only the specified folder. If you select this option, you need to specify a folder path.

Step 5.

> This step is available if you selected the following category type: **Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category**.

In this step, specify the folder whose executable files will be used to create the category.

Manage the following settings:

- **Include dynamic-link libraries (DLL) in this category**

  The application category includes dynamic-link libraries (files in DLL format), and the Application Control component logs the actions of such libraries running in the system. Including DLL files in the application category may reduce the performance of Kaspersky Security Center.

  This check box is cleared by default.

- **Include script data in this category**

  The application category includes data on scripts, and scripts are not blocked by Web Threat Protection. Including the script data in the category may lower the performance of Kaspersky Security Center.

  This check box is cleared by default.

- **Algorithm for hash function calculation**

  Depending on the version of the security application installed on devices in your network, you need to select a hashing algorithm that Kaspersky Security Center applies to files in the category. Information about hash values calculated by hash functions is stored in the database of the Administration Server.

  SHA256 is a cryptographic hash function whose algorithm has no known weaknesses; it is currently considered the most secure hash function. Kaspersky Endpoint Security for Linux supports SHA256.

Select one of the hashing algorithm to apply to files in the category:

- If you are using Kaspersky Endpoint Security for Linux on the protected devices, select the **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)** check box.

- If you are using Kaspersky Endpoint Security for Windows on the protected devices, select the **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** check box.

If you are using the applications both for Windows and Linux on your network, select both check boxes.

- **Force folder scan for changes**

  If this option is enabled, the application regularly checks the folder of category content addition for changes. You can specify the frequency of checks (in hours) in the entry field next to the check box. By default, the time interval between forced checks is 24 hours.

  f this option is disabled, the application does not force any checks of the folder. The Server attempts to access files if they have been modified, added, or deleted.

  This check box is cleared by default.

Step 6.

Finish the wizard. When the wizard finishes, the new application category is created. You can control application from the category using Application Control rules.

Golden Image

You can use the Inventory to add the Golden Image application category. By default, the category is empty. The "Golden Image" category includes applications that are delivered to the device along with the operating system. Applications in this category are considered trusted. If necessary, you can add third-party applications to the category.

Upon completion of the Inventory task, the application can modify the "Golden Image" category as follows:

- **No changes** – do not change the Golden Image category after completing the inventory. This is the default selection. This option is used when you want to get a list of third-party applications used on the device, but not to add them to the "Golden Image" category.

- **Update or create (if does not exist)** – adds applications detected on the device by the inventory task to the "Golden Image" category. If the category does not exist, it is created. If the category exists, the list of applications in the category is updated.

- **Remove** – clear the Golden Image application category. The category is cleared immediately the task is started, without doing an inventory of files on the device.

This can be useful in the following scenarios:

- If you need to prevent the launch of applications from the "Golden Image" category on the device, but you cannot disable the Application Control rule.
- If you apply a new policy to a device that contains Application Control rules that differ from the current policy, or when you move a device to a child policy. In this case, we recommend clearing the "Golden Image" category to avoid blocking allowed applications by mistake.

Configuring a Golden Image category based on a baseline computer

You can use a baseline computer to create a Golden Image category with a set of applications that you need. You can then use this category to create Application Control allow rules.

Configuring a Golden Image category based on a baseline computer involves the following steps:

1. **Configure a reference computer**

   Install and configure all the software that you need for the devices to work on the corporate network, including Kaspersky Endpoint Security for Linux and Network Agent.

2. **Create an Inventory task**

   Create the task in the Web Console or on the command line and manage the following settings:

   - Action with the "Golden Image" category of applications: **Update or create (if does not exist)**;

     ```
     GoldenImageAction=Create
     ```

   - The inventory scope is the reference computer.

3. **Run the Inventory task and wait for it to complete.**

   The task generates the "Golden Image" category of applications.

4. **Export the list of categories to a file.**

   > You cannot export a list of categories in the Web Console.

   Execute the command:

   ```
   kesl-control [-A] --get-categories --file <path to file> --json
   ```

   Where `<path to file>` is the path to the configuration file to which you want to output the task settings.

5. **If necessary, adjust your "Golden Image" category**

   Review the configuration file with the list of application categories. If necessary, adjust the list of applications in the "Golden Image" category.

6. **Import settings from the configuration file.**

   If you have modified the configuration file with the list of application categories, import it into the application:

   ```
   kesl-control [-A] --set-categories --names GoldenImage [<category name 1> <category name 2> ... <name of category N>] --file <path to file>
   ```

   where `<category name 1> <category name 2> ... <category name N>` are names of the categories other than the "Golden Image" category, the information about which categories you want to change.

   `<path to file>` is the path to the configuration file to which you want to output the task settings.

As a result, you can use the "Golden Image" category to create Application Control rules.

About Application Control rules

An *Application Control rule* is a set of conditions that determine whether Application Control allows or denies the launch of a third-party application for a selected group of users.

The rules restrict the launch of third-party applications in accordance with the following criteria:

- **Application categories**. The application belonging to the application category.

  > Each category can only be used in one rule.

- **Users and user groups**. Application Control allows restricting access to third-party applications for individual users or user groups. For example, you can restrict access to remote administration applications for all users in the organization except those in the IT department.

Application control rules can have one of the following *operation statuses*:

- **Enabled**. Application Control applies the rule.
- **Disabled**. Application Control does not apply the rule.
- **Test**. Application Control will not block third-party applications from running, but will send notifications about their launch to the Administration Server.

How to add Application Control rules in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **App Control**.
5. Make sure the toggle switch for the component is in the **App Control ENABLED** position.
6. In the **Action on starting applications** block, click the **Add** button.

   This opens the form for adding an Application Control rule.

7. In the **Status** field, set the status of the rule.

8. If you want test the rule, set this toggle switch to **Enabled** and select the **Test mode** check box.

9. In the **Rule name** field, enter the rule name. The rule name must be unique.

10. Select the category of applications to which you want to apply the rule. A rule cannot be saved without specifying a category.

11. Select users or a group of users and their permissions to run applications.

12. To apply the policy to computers, close the padlock icons and save your changes.

How to add Application Control rules on the command line

1. Output the list of Application Control rules to a file:

```
kesl-control --get-settings 21 --file <path to file> [--json]
```

2. Open the configuration file and add a section for the rule with ID `#`, depending on the Application Control mode:

   a. If the `AppControlMode=AllowList`:

   ```
   [AllowListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [AllowListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   mode is selected

   b. If the `AppControlMode=DenyList`:

   ```
   [DenyListRules.item_#]
   Description=<rule name>
   AppControlRuleStatus=<On|Off|Test>
   Category=<category name>
   [DenyListRules.item_#.ACL.item_#]
   Access=<Allow|Block>
   Principal=<user>
   ```

   mode is selected

3. Import the settings from the configuration file into the application:

```
kesl-control --set-settings 21 --file <path to file> [--json]
```

Symbols

Command options

Setting	Description
`[AllowListRules.item_#]` `[DenyListRules.item_#]`	Application control rule with ID `#`.
`[AllowListRules.item_#.ACL.item_#]` `[DenyListRules.item_#.ACL.item_#]`	List of users to which the Application Control rule with ID `#` applies.
`Description`	Description of the Application Control rule.
`AppControlRuleStatus`	Operation status of the Application Control rule: `On` (default value): the rule is enabled, Kaspersky Endpoint Security applies this rule for the Application Control. `Off`: the rule is not used for the Application Control. `Test` – Kaspersky Endpoint Security allows applications covered by the rule to be launched, but logs information about the launch of these applications in the report.
`Category`	Name of the application category for which the rule applies. You can specify the `Golden Image` category.
`Access`	Access type assigned to a user or user group: `Allow` (default value) — Allow running applications. `Block` – Deny running applications.
`Principal`	User or user group to which the Application Control rule applies: `\Everyone` (default value): the rule applies to all users. `<user>` is the name of the user to which the rule applies. `@<group name>` is the name of the group of users to which the rule applies.

Application Control rules test mode

To ensure that Application Control does not block applications necessary for the operation, it is recommended that you test the Application Control rules. In testing mode, Kaspersky Endpoint Security blocks third-party applications from running and sends notifications about their launch to the Administration Server.

By default, Application Control allows all third-party applications to run, except those prohibited by the rules.

Testing Application Control rules

1. **Create the Application Control rules**

   Configure and enable Application Control rules that you want to test. For example, you can create rules that prevent execution of any third-party applications, except for applications from the "Golden Image" and "Work applications" categories.

2. **Enable Application Control in test mode**

   How to enable the Test mode of Application Control in the Web Console

   1. In the main window of the Web Console, select **Asset management** → **Policies**.
   2. Click the name of the Kaspersky Endpoint Security policy.

      The policy properties window opens.
   3. Select the **Application settings** tab.

4. Go to **Security Controls** → **App Control**.

5. Make sure the toggle switch for the component is in the **App Control ENABLED** position.

6. Under **Action on starting applications**, select the **Inform** action for Application Control.

7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to enable the Test mode of Application Control on the command line

To select the test mode for Application Control, run the following command:

```
kesl-control --set-settings 21 AppControlRulesAction=TestRules
```

3. **Review the test results**

Review the Application Control report and events of the component, which are sent to Kaspersky Security Center.

How to view the Application Control report in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Security Controls** → **App Control**.

5. Make sure the toggle switch for the component is in the **App Control ENABLED** position.

6. In the table with Application Control rules, click the **View report** button.

7. The **Report on prohibited applications in test mode** window opens.

8. Review the information about the prohibited applications starting in testing mode.

How to view events resulting from a test run of Application Control

1. In the main window of the Web Console, select **Monitoring** → **Event selections**.

2. Click **Add**.

3. In the opened **New event selection** window, specify a name for the selection. For example, "Testing of Application Control rules".

4. Go to the **Events** section and manage the following settings:

   - **Application name** – Kaspersky Endpoint Security for Linux.

   - **Severity level** – **Info**.

- Select the **Include selected general events** option.
- Select the check boxes opposite the **Application startup prohibited in test mode** and **Application startup allowed in test mode** events.

5. If necessary, configure the remaining settings.
6. Save your changes.
7. Click the name of the selection to view the result of the selection of events.

4. **Adjust the rules**

   If test mode results in no blocked startup events for all applications required for the work of the computer user, this means that the correct rules were created.

   Otherwise, edit the settings of the rules you have created, create additional rules, or delete the existing rules.

System Integrity Monitoring

The System Integrity Monitoring component monitors changes in the operating system that may indicate computer security breaches. When such changes are detected, Kaspersky Endpoint Security generates corresponding events and alerts the administrator.

How System Integrity Monitoring works

System Integrity Monitoring can work in real time and on demand:

- The *System Integrity Monitoring* component allows you to monitor changes in the files and directories you have included in the monitoring scope *in real time*.
- The *System Integrity Check* feature allows you to compare the current status of objects included in the monitoring scope with their recorded status, either *on a schedule or on demand*.

System Integrity Monitoring does not share data on exact changes that were made. The *System Integrity Check* task sends data on modified attributes, and moved files and directories.

Special considerations and limitations

- The technical limitations of the Linux operating system prevent the application from identifying the user or process that made the changes to the file.
- When a directory is added to a monitoring or exclusion scope, the application does not check whether that directory exists.

Real-time System Integrity Monitoring

System Integrity Monitoring allows real-time detection of changes of an object included in the monitoring scope.

How System Integrity Monitoring works

1. **The application intercepts file operation events**

   The application uses a special interception mechanism that has read-only access to a file being scanned.

2. **The application checks the file to see if it has been modified.**

   System Integrity Monitoring tracks changes in the following file properties:

   - Content (`write ()`, `truncate ()` and other modifications)
   - Metadata (changing access permissions with `chmod` or `chown` commands)
   - Time stamps (`utimensat`)
   - Extended attributes (`setxattr`) and others

3. **Completion of the scan**

   The application generates a *System integrity check failed* event if the file has been modified.

Configuring System Integrity Monitoring

1. **Enable System Integrity Monitoring**

   System Integrity Monitoring is disabled by default. Pick devices for which you want to monitor file changes in real time, and enable the System Integrity Monitor component on these devices.

2. **Configure monitoring scope**

   For the component to work, at least one monitoring scope must be specified. The *Kaspersky internal objects* (`/opt/kaspersky/kesl/`) monitoring scope is set by default.

   Kaspersky Endpoint Security scans objects in the specified scopes, in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

   How to configure a monitoring scope in the Web Console

   1. In the main window of the Web Console, select **Asset management** → **Policies**.
   2. Click the name of the Kaspersky Endpoint Security policy.

      The policy properties window opens.
   3. Select the **Application settings** tab.

4. Go to **Security Controls** → **System Integrity Monitoring**.

5. Click the **Monitoring scopes** link.

   This opens a window with a table of scan scopes.

6. Click **Add**.

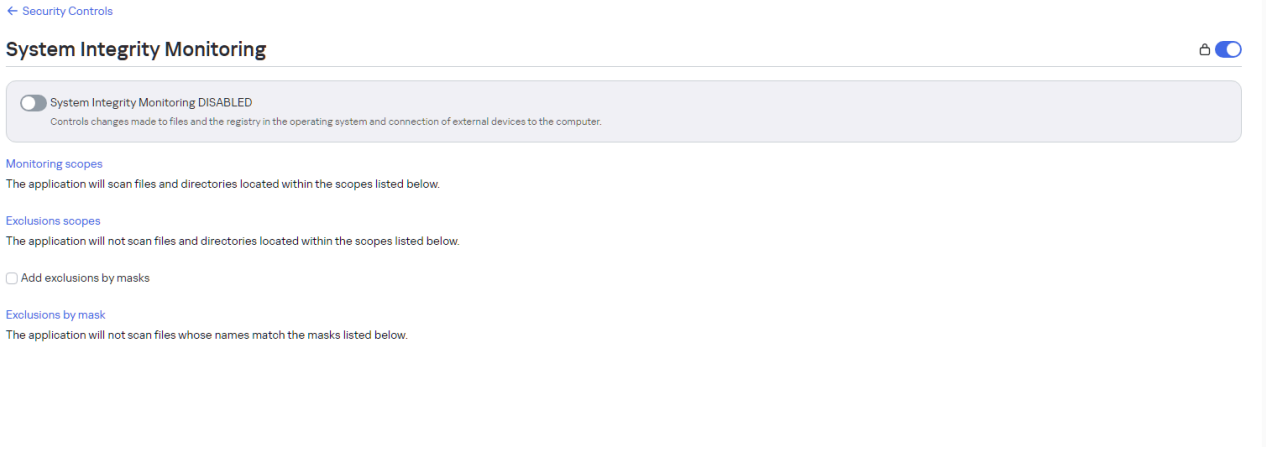
   This opens the window for adding scan scopes

7. In the **Name** field, specify the name of the monitoring scope, for example, *Critical objects*.

8. In the **Path** field, specify the path to an individual file or directory (for example, `/path/to/folder`). Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

9. If necessary, specify masks for object names in the command shell format (for example, `*.txt` or `file?.*`). Add masks one at a time.

10. To apply the policy to computers, close the padlock icons and save your changes.



System Integrity Monitoring

How to configure a monitoring scope on the command line

1. Run the following command:

```
kesl-control --set-settings 11  ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 11
```

Symbols

Command options

Setting	Description
`UseScanArea=Yes`	Enabling a monitoring scope with an `#` ID. You can temporarily disable a monitoring scope scan instead of deleting the scope. To do this, set `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description of monitoring scope; contains additional information about the monitoring scope.

Setting	Description
`AreaMask.item_#`	Monitoring scope limitation. Within the monitoring scope, the application scans only the objects that are specified using the masks in the shell format. For example, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Path to the monitoring directory. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

Example

A monitoring scope that includes only the `/etc` directory:

```
kesl-control --set-settings 11 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

3 Configure exclusion scopes

An exclusion has a higher priority than a monitoring scope. An excluded object is not scanned even if it is in a monitoring scope. If the monitoring scope is defined on a lower level than the excluded directory, the application skips this monitoring scope during system integrity monitoring.

How to configure an exclusion scope in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Security Controls** → **System Integrity Monitoring**.

You can specify exclusions by path or by the file name mask. The application can exclude an entire directory (or an individual file) from scanning, or exclude files with a matching name mask in monitoring scopes.

To add exclusions by path:

1. Click the **Exclusions scopes** link.

   This opens a window with a table of exclusion scopes.
2. Click **Add**.

   This opens the window for adding exclusion scopes.
3. In the **Name** field, specify the name of the exclusion scope, for example, *System files*.
4. In the **Path** field, specify the path to an individual file or directory (for example, `/path/to/folder`). Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.
5. Specify masks of object names in the command shell format (for example, `*.txt` or `file?.*`). Add masks one at a time.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

To add exclusions by file name mask:

1. Select the **Add exclusions by masks** check box.
2. Click the **Exclusions by mask** link.

   This opens a table with exclusion scopes by mask.
3. Click **Add**.

   This opens the window for adding exclusion scopes by mask.
4. Specify the file name mask in the command shell format (for example, `*.txt` or `file?.*`). Add masks one at a time.
5. To apply the policy to computers, close the padlock icons and save your changes.

How to configure an exclusion scope on the command line

1. Run the following command:

```
kesl-control --set-settings 11  ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 11
```

Symbols

Command options

Setting	Description
`UseScanArea=Yes`	Excludes the specified scope from monitoring with the `#` ID. You can temporarily disable an exclusion scope instead of deleting the scope. To do this, set `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description of the monitoring exclusion scope, which contains additional information about the monitoring exclusion scope.
`AreaMask.item_#`	Limitation of the exclusion scope. In the exclusion scope, the application excludes from scans only the objects specified using masks in the shell format. For example, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	The path to the directory to be excluded from scanning. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

Example

An exclusion scope that includes only the `/tmp` directory:

```
kesl-control --set-settings 11 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

System Integrity Check

While running the *System Integrity Check* task, the application compares the current state of each object with its original state, or baseline. The baseline contains paths to monitored objects and their metadata. This allows tracking changes in files and directories included in the monitoring scope.

A baseline may also contain personal data.

In contrast to the System Integrity Monitoring component, the *System Integrity Check* task helps limit the number of events and lets you generate a summary report of changes in the operating system.

How the System Integrity Check works

1. **The application takes a snapshot of the system**

   The system baseline is created during the first run of the task. If you have created multiple System Integrity Check tasks, a separate baseline is created for each. For Linux devices, a baseline is rebuilt when task settings change, for example, if a new monitoring scope is added, as well as when the task is started with the **Rebuild baseline on each task start** setting enabled.

   The storage for baselines is located in `/var/opt/kaspersky/kesl/private/fim.db`. Root privileges are required to access a database that contains baselines. The baseline is deleted together with the associated System Integrity Check task.

2. **The application looks for changes in the state of the system**

   The application applies the following criteria to compare information about objects included in the monitoring scope:

   - SHA256 hash of the file (for a full check)
   - File change time
   - File size

3. **Completion of the scan**

   If the current state of the system differs from the baseline, Kaspersky Endpoint Security generates a system integrity violation event: *System integrity check failed*.

Configuring and running the System Integrity Check task

1. **Create a System Integrity Check task**

   How to create the System Integrity Check task in the Web Console

   1. In the main window of the Web Console, select **Tasks**.

      The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux 12.5**.

   b. In the **Task type** drop-down list, select **System Integrity Check**.

   c. In the **Task name** field, enter a brief description, for example, *Weekly System Integrity Check*.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option.

5. Finish the wizard.

How to create the System Integrity Check task on the command line

To create a task, run the following command:

```
kesl-control --create-task <task name> --type ODFIM
```

where `<task name>` is the name of the new task.

This command returns the ID of the created task.

Example of the command execution result:

Task created (task ID: 115)

2. **If necessary, edit the task settings**

How to configure the System Integrity Check task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the newly created System Integrity Check task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Select the scan type:

   - **Full Scan**. The application compares the SHA256 hash of the file in its current state with the hash from the system snapshot.

   - **Quick Scan**. The application only compares file sizes. If the file size has not changed, the modification time is not considered a critical parameter.

5. In the **System Integrity Check settings** section, select check boxes:

   - **Rebuild baseline on each task start**. If this check box is selected, the application rebuilds the baseline each time the task is started.

   - **Track directories in monitoring scopes**. If this checkbox is selected, the application checks the directories specified by the user. If the check box is cleared, the application scans the default scan scope only – *Kaspersky internal objects* (`/opt/kaspersky/kesl/`).

   - **Track the last time a file was accessed on each task start**. If this checkbox is selected, the application checks the last access time of the file (the `noatime` parameter) every time the task runs.

6. Save your changes.

How to configure the System Integrity Check task on the command line

Execute the command:

```
kesl-control --set-settings <task ID|name> RebuildBaseline=<Yes|No> [CheckFileHash=<Yes|No>]
[TrackDirectoryChanges=<Yes|No>] [TrackLastAccessTime=<Yes|No>] [UseExcludeMasks=<Yes|No>]
[ExcludeMasks.item_#=<object mask>]
```

Symbols

System Integrity Check task settings

Setting	Description
`RebuildBaseline`	Rebuild baseline on each task start.
`CheckFileHash`	Scan of the SHA256 hash of the file. If this check is disabled, the application compares only the file size (if the file size has not changed, then the modification time is not considered a critical parameter).
`TrackDirectoryChanges`	Scanning directories specified by the user. If the setting is disabled, the application only scans the default scope (`/opt/kaspersky/kesl/`).
`TrackLastAccessTime`	Checking the last access time for the file (`noatime` option).
`UseExcludeMasks`	Monitoring exclusions. A new `[ExcludeMasks.item_#]` section will be added to the task settings. The application will not scan the objects specified in this section. This setting applies only if the `ExcludeMasks.item_#` setting is specified.
`ExcludeMasks.item_#=<object mask>`	Excluding of objects from the monitoring scope. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in command shell format. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask. This setting can be managed only if the `UseExcludeMasks` parameter is enabled. You can specify several masks. Each mask must be specified on a new line with a new index. Example: `ExcludeMasks.item_0000=<eicar1.*>`

3 Configure monitoring scope

At least one monitoring scope must be specified for the task to start. The *Kaspersky internal objects* (`/opt/kaspersky/kesl/`) monitoring scope is set by default.

The task is only run if the baseline contains information about objects that belong to the monitoring scope of the task.

Kaspersky Endpoint Security scans objects in the specified scopes, in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

How to configure a monitoring scope in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click the newly created System Integrity Check task.

   The task properties window opens.

3. Select the **Application settings** tab.

4. Make sure the **Track directories in monitoring scopes** check box is selected.

5. In the **Monitoring and exclusions scopes** block, click the **Monitoring scopes** link.

   This opens a window with a table of scan scopes.

6. Click **Add**.

   This opens the window for adding scan scopes

7. In the **Name** field, enter a name for the monitoring scope, for example, *Files on the desktop*.

8. In the **Path** field, specify the path to an individual file or directory (for example, `/path/to/folder`). Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

9. If necessary, specify masks for object names in the command shell format (for example, `*.txt`, `file?.*`). Add masks one at a time.

10. Save your changes.

How to configure a monitoring scope on the command line

1. Run the following command:

```
kesl-control --set-settings <task ID|name> TrackDirectoryChanges=Yes ScanScope.item_#.UseScanArea=Yes
        [ScanScope.item_#.AreaDesc=<description of the area>\]
        [ScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ScanScope.item_#.Path=<path to the directory>
```

2. To check the current settings, run the following command:

```
kesl-control --get-settings <task ID|name>
```

Symbols

System Integrity Check task settings

Setting	Description
`UseScanArea=Yes`	Enabling a monitoring scope with an `#` ID. You can temporarily disable a monitoring scope scan instead of deleting the scope. To do this, set `ScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description of monitoring scope; contains additional information about the monitoring scope.
`AreaMask.item_#`	Monitoring scope limitation. Within the monitoring scope, the application scans only the objects that are specified using the masks in the shell format. You can specify several `ScanScope.item_#.AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order. For example, `ScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	Path to the monitoring directory. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

Example

A monitoring scope that includes only the `/etc` directory:

```
kesl-control --set-settings 115 ScanScope.item_0000.UseScanArea=Yes ScanScope.item_0000.Path=/etc
```

4 **Configure exclusion scopes**

An exclusion has a higher priority than a monitoring scope. An excluded object is not scanned even if it is in a monitoring scope. If the monitoring scope is defined on a lower level than the excluded directory, the application skips this monitoring scope during system integrity monitoring.

How to configure an exclusion scope in the Web Console

1. In the main window of the Web Console, select **Tasks**.
2. The list of tasks opens.
3. Click the newly created System Integrity Check task.

   The task properties window opens.
4. Select the **Application settings** tab.

You can specify exclusions by path or by the file name mask. The application can exclude an entire directory (or an individual file) from scanning, or exclude files with a matching name mask in monitoring scopes.

To add exclusions by path:

1. In the **Monitoring and exclusions scopes** block, click the **Exclusions scopes** link.

   This opens a window with a table of exclusion scopes.
2. Click **Add**.

   This opens the window for adding exclusion scopes.
3. In the **Name** field, specify the name of the exclusion scope, for example, *System files*.
4. In the **Path** field, specify the path to an individual file or directory (for example, `/path/to/folder`). Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.
5. Specify masks of object names in the command shell format (for example, `*.txt` or `file?.*`). Add masks one at a time.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

To add exclusions by file name mask:

1. In the **Monitoring and exclusions scopes** block, click the **Exclusions by mask** link.

   This opens a table with exclusion scopes by mask.
2. Click **Add**.

   This opens the window for adding exclusion scopes by mask.
3. Specify the file name mask in the command shell format (for example, `*.txt` or `file?.*`). Add masks one at a time.
4. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to configure an exclusion scope on the command line

1. Run the following command:

```
kesl-control --set-settings <task ID|name>      ExcludedFromScanScope.item_#.UseScanArea=Yes
        [ExcludedFromScanScope.item_#.AreaDesc=<description of the area>\]
        [ExcludedFromScanScope.item_#.AreaMask.item_#=<mask in shell format>\]
        ExcludedFromScanScope.item_#.Path=<path to the directory>
```

2. To check the current settings, run the following command:

```
kesl-control --get-settings <task ID|name>
```

Symbols

System Integrity Check task settings

Setting	Description
`UseScanArea=Yes`	Excludes the specified scope from monitoring with the `#` ID. You can temporarily disable an exclusion scope instead of deleting the scope. To do this, set `ExcludedFromScanScope.item_#.UseScanArea=No`.
`AreaDesc`	Description of the monitoring exclusion scope, which contains additional information about the monitoring exclusion scope.
`AreaMask.item_#`	Limitation of the exclusion scope. In the exclusion scope, the application excludes from scans only the objects specified using masks in the shell format. You can specify several `ExcludedFromScanScope.item_#.AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order. For example, `ExcludedFromScanScope.item_0001.AreaMask.item_0001=*.exe` `ScanScope.item_0001.AreaMask.item_0002=*.txt`.
`Path`	The path to the directory to be excluded from scanning. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

Example

An exclusion scope that includes only the `/tmp` directory:

```
kesl-control --set-settings 115 ExcludedFromScanScope.item_0001.UseScanArea=Yes
ScanScope.item_0001.Path=/tmp
```

5 Run the task

How to run the System Integrity Check task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Select the check box next to the created task.

3. Click **Start**.

How to run the System Integrity Check task on the command line

To run the task, run the following command:

```
kesl-control --start-task <task ID|name> [-W] [--progress]
```

where:

- `<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.
- `[-W]` enables the output of current events related to this task.
- `[--progress]` enables the display of task progress.

Trusted zone

A *trusted zone* is a system administrator-configured list of objects and applications that Kaspersky Endpoint Security does not monitor when active.

The administrator forms the trusted zone independently, taking into account the features of the objects that are handled and the applications that are installed on the computer. It may be necessary to include objects and applications in the trusted zone when Kaspersky Endpoint Security blocks access to a certain object or application, if you are sure that the object or application is harmless.

Trusted zone settings

Settings	Description
Web addresses	Web addresses that the Web Threat Protection component considers trusted. The component does not scan incoming and outgoing traffic from these addresses for threats. The list of trusted addresses can be used, for example, if the component interferes with downloading a file from a known website. For more information, see the How to add trusted web addresses article
IP addresses	IP addresses of trusted devices. The Network Threat Protection component does not block network activity from these addresses. The application also does not log information on network attacks from the IP addresses that are in the list of exclusions. For more information, see the How to add a trusted IP address of a computer article
Network ports	The list of network ports that the Network Threat Protection component excludes from scanning. For more information, see the How to select monitored network ports article
Root certificates	Root certificates that Kaspersky Endpoint Security considers trusted. The list of trusted root certificates is used when the Web Threat Protection, Mail Threat Protection, and Web Control components scan encrypted connections (HTTPS connections). For more information, see the How to add a certificate to the list of trusted root certificates article
Domains	List of trusted domains. The Web Threat Protection and Web Control components do not control encrypted connections with these domains. For more information, see the How to add a trusted domain article
Mount points	List of trusted mount points. The File Threat Protection, Anti-Cryptor, and Container Scan components exclude the specified mount points from scanning. Mount points must be specified in the same way as they are displayed in the `mount` command output. For more information, see the How to exclude mount points article
Applications	Applications for which Kaspersky Endpoint Security does not control file and network activity or system registry access. Protection components such as File Threat Protection or Behavior Detection will not control the activity of the specified applications. For more information, see the How to add trusted applications article

Settings	Description
Malware Scan exclusions	Files or folders, as well as object types (according to the Virus Encyclopedia) that are excluded from scanning by all or some of the application components. For more information, see the How to add protection exclusions article
Devices	Devices to which the Device control component always allows full access for selected users or groups. For more information, see the How to add trusted devices article

How to add protection exclusions

A *protection exclusion* is a set of conditions under which Kaspersky Endpoint Security will not scan objects for viruses and other malware.

You can exclude objects from scans by using the following methods:

- **Exclusions**. Directory path. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask. Example: `/.snapshots/*/snapshot/`.

  To specify paths in containers or images, use tags.

  How to use tags

  You can use special tags to specify a container or image:

  - `[container-id:<id>]/<path to local directory>`
  - `[container-name:<name>]/<path to local directory>`
  - `[image-id:<id>]/<path to local directory>`
  - `[image-name:<name>]/<path to local directory>`

  Where:

  `<id>` is the container ID.

  `<name>` is a container name

  `<path to local directory>` is the path to the local directory.

  You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

  Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

  For example:

  - `[container-name:<name>][image-name:<name>]/path to local directory>`
  - `[container-id:<id>][image-name:<name>]/<path to local directory>`
  - `[image-name:<name>][image-id:<id>]/<path to local directory>`

- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`

- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

- **Exclusions by mask**. File name specified with a mask. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask. Example: the `*.txt` mask captures all text files.

  Use masks:

  - The `*` (asterisk) character, which takes the place of any set of characters, except the `\` and `/` characters (delimiters of the names of files and directories in paths to files and directories). For example, the mask `/dir/*/*.txt` will include all paths to files with the TXT extension located in directories within the dir directory, but not in subdirectories.

  - Two consecutive `*` characters take the place of any set of characters (including an empty set) in the file or directory name, including the `\` and `/` characters (delimiters of the names of files and directories in paths to files and directories). For example, the mask `/dir/**/*.txt` will include all paths to files with the TXT extension located in directories nested within the dir directory, excluding the dir directory itself.

  - The `?` (question mark) character, which takes the place of any single character, except the `\` and `/` characters (delimiters of the names of files and directories in paths to files and directories). For example, the `/dir/???.txt` mask will include paths to all files residing in the dir directory that have the TXT extension and a name consisting of three characters.

- **Exclusions by threat name** Name of the object type according to the classification of the Kaspersky Encyclopedia (for example, `Email-Worm`, `Rootkit`, or `RemoteAdmin`). You can use masks with the `?` character (replaces any single character) and the `*` character (replaces any number of characters). For example, if the `Client*` mask is specified, the application excludes `Client-IRC`, `Client-P2P` and `Client-SMTP` objects from scans.

- **Exclusions by process** Process path.

Kaspersky Endpoint Security also allows excluding files of certain formats: archives, email databases, text files, database log files.

How to add protection exclusions in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Host Threat Protection** → **File Threat Protection**.

5. Click the **Scan exclusions** link.

6. In the window that opens, click the **Add** button.

7. Select check boxes for criteria that you want to use for an exclusion from protection:

   - **Path to the file or folder**. Specify a file or directory path or a file name mask. To specify paths in containers or images, use tags.

     For a local file system, specify a directory path (for example, `/path/to/folder/`). For a mounted file system or all remote mounted file systems, enter a file name mask. For a mounted file system, also specify the access protocol (NFS, Samba, or custom).

   - **Object type**. Specify the threat name.

   - **Object hash**. Enter the SHA256 hash of the object. You can also add a file or specify an event from which to derive the SHA256 hash for the exclusion.

8. Select the protection components to which you want to apply the exclusion:

   - **All protection components**. The exclusion is applied to all protection components that are affected by **Malware Scan exclusions**.

   - **Selected protection components**. Select the components to which you want to apply the exclusion: File Threat Protection, Anti-Cryptor, Exploit Prevention.

9. To apply the policy to computers, close the padlock icons and save your changes.

How to add protection exclusions on the command line

1. To add an exclusion by path, run the following command:

```
kesl-control --set-settings 1 --add-exclusion <path>
```

2. To add an exclusion by mask, follow these steps:

   a. Enable file exclusion by mask:

```
kesl-control --set-settings 1 UseExcludeMasks=Yes
```

   b. Add a file mask:

```
kesl-control --set-settings 1 ExcludeMasks.item_#=<file mask>
```

3. To add an exclusion by threat name, follow these steps:

   a. Enable file exclusion by threat name:

```
kesl-control --set-settings 1 UseExcludeThreats=Yes
```

   b. Add a threat name:

```
kesl-control --set-settings 1 ExcludeThreats.item_#=<threat name>
```

4. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 1
```

Symbols

Command options

Setting	Description
`--add-exclusion`	Exclude a directory from scanning. A new `[ExcludedFromScanScope.item_#]` section will be added to the task settings. The application will exclude objects in the directory specified by the `path` setting from scans.
`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. Use masks in the shell format to enter the file name. Example: `ExcludeMasks.item_0000=*_my_file_??.html`.
`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected. For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans. Example: `ExcludeThreats.item_0000=EICAR-Test-*`.

How to add trusted web addresses

In addition to malicious and phishing websites, Web Threat Protection can block other websites. For example, Web Threat Protection blocks HTTP traffic that does not satisfy RFC standards. You can create a list of URLs whose content you trust. The Web Threat Protection component does not analyze information from trusted web addresses to check them for viruses or other threats. This option may be useful, for example, if the Web Threat Protection component interferes with downloading a file from a known website.

How to add a trusted web address in the Web Console

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Trusted Zone** section.
5. In the window that opens, click the **Web addresses** link.

   This opens a window containing a list of truste web addresses.
6. Create a list of URLs / web pages whose content you trust.

   Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.

   You can also import a list of trusted web addresses from a JSON file.
7. To apply the policy to computers, close the padlock icons and save your changes.

How to add a trusted web address on the command line

1. To enable the list of trusted web addresses, run the following command:

```
kesl-control --set-settings 14 UseTrustedAddresses=Yes
```

2. To add a trusted web address, run the following command:

```
kesl-control --set-settings 14 TrustedAddresses.item_#=<trusted web address>
```

3. To check the current values of the component settings, run the following command:

```
kesl-control --get-settings 14
```

Example

```
kesl-control --set-settings 14 TrustedAddresses.item_001=https://example.com/
```

How to add a trusted IP address of a computer

Kaspersky Endpoint Security can recognize a network attack and block an unsecured network connection that is transmitting a large number of packets (for example, from surveillance cameras). To work with trusted devices, you can add the IP addresses of these devices to the list of exclusions. Trusted web addresses affect the Network Threat Protection component.

How to configure addresses excluded from blocking in the Web Console

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **Trusted Zone** section.
5. In the window that opens, click the **IP addresses** link.
   This opens a window containing a list of trusted IP addresses.
6. In the window that opens, click the **Add** button.
7. Enter the IP address of the computer from which network attacks must not be blocked.
   If necessary, specify the subnet.
8. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to configure addresses excluded from blocking on the command line

1. To apply trusted IP addresses, run the following command:

```
kesl-control --set-settings 17 UseExcludeIPs=Yes
```

2. To add a trusted IP address, run the following command:

```
kesl-control --set-settings 17 ExcludeIPs.item_#=<IP address>
```

3. To scan the list of trusted IP addresses, run the following command:

```
kesl-control --get-settings 17 TrustedIPAddresses
```

Example

```
kesl-control --set-settings 17 ExcludeIPs.item_0000="192.168.2.0/24"
```

How to select monitored network ports

Kaspersky Endpoint Security monitors data streams that are transmitted via certain protocols and pass through certain open TCP ports on user's computer. By default, the application monitors known and registered ports, for example, port 443 for HTTPS connections, port 143 for the IMAP mail protocol.

Trusted network ports are network ports that the Network Threat Protection component excludes from scanning. This is necessary to configure Kaspersky Endpoint Security for compatibility with trusted third-party services and applications, as well as to optimize performance. For example, you can specify network ports for internal backup services so that the application does not interfere with downloading or uploading backup copies.

It is important to remember that excluding network ports from scanning makes a device less protected. Try to keep exclusions to a minimum.

How to exclude network ports from scanning in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Trusted Zone** → **Network ports**.

   This opens a window containing a list of monitored network ports.

5. Disable the toggle switch for the ports that you want to exclude from scanning.

   If the port that you need is not listed, it means the application does not scan that port.

6. To apply the policy to computers, close the padlock icons and save your changes.

How to exclude network ports from scanning on the command line

1. Get a list of monitored ports by running the following command:

   ```
   kesl-control --get-net-setting
   ```

2. If monitoring of all ports is enabled (`MonitorNetworkPorts=All`), run the following command:

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=Selected
   ```

   This adds a `[NetworkPorts.item_#]` section containing monitored network ports.

3. If the section contains a port that you want to exclude from scanning, follow these steps:

   a. To output network traffic scan settings to a file, run the following command:

   ```
   kesl-control --get-net-setting --file <path to file>
   ```

   b. In this file, delete the `[NetworkPorts.item_#]` sections containing network ports that you do not want to be monitored.

   c. To apply your settings, run the following command:

   ```
   kesl-control --set-net-settings --file <path to file>
   ```

   Modified settings are imported into the application.

How to add a certificate to the list of trusted root certificates

Kaspersky Endpoint Security lets you install trusted root certificates on user computers if, for example, you need to deploy a new certification center. The application lets you add a certificate to a special Kaspersky Endpoint Security certificate store. In this case, the certificate is considered trusted only for the Kaspersky Endpoint Security application. In other words, the user can gain access to a website with the new certificate in the browser. If another application tries to gain access to the website, you can get a connection error because of a certificate issue.

Trusted root certificates are used by the following components:

- Web Threat Protection
- Mail Threat Protection
- Web Control

Trusted certificates in CER, CRT, PEM and DER formats are supported. The maximum file size for a trusted certificate is 2 MB.

How to install a trusted root certificate in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Trusted Zone** → **Root certificates**.
   This opens a window containing a list of trusted root certificates.
5. Click **Add**.
   This opens the form for adding a certificate.
6. Upload the certificate.
7. If necessary, enter a description of the certificate in the **Comment** field.
8. Save your changes.

In the list of trusted certificates, the serial number is used as the certificate name.

How to install a trusted root certificate on the command line

1. To add a certificate, run the following command:

   ```
   kesl-control --add-certificate <path to certificate>
   ```

2. To view the list of trusted root certificates, run the following command:

   ```
   kesl-control --list-certificates
   ```

   The following information is displayed for each certificate:

   - Certificate subject
   - serial number
   - Certificate issuer
   - Certificate start date
   - Certificate expiration date
   - SHA256 certificate fingerprint

3. To remove a certificate from the list, run the following command:

   ```
   kesl-control --remove-certificate <certificate subject>
   ```

How to add a trusted domain

Kaspersky Endpoint Security has a list of trusted domains for which it does not scan encrypted connections. Trusted domains affect Web Threat Protection and Web Control. Excluding domains from scanning lets you avoid blocking traffic from sources that you know.

Specify the domain name. Web addresses, such as `example.com/*` or `https://example.com` are ignored.

How to specify trusted domains in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Trusted Zone** → **Trusted domains**.

   This opens a window containing a list of trusted domains.
5. Click **Add**.

   This opens the form for adding a domain.
6. Specify a domain name or domain mask. For example, `*example.com`.
7. Save your changes.

How to specify trusted domains on the command line

1. To add a domain, run the following command:

   ```
   kesl-control --set-net-settings ManageExclusions=Yes Exclusions.item_#.DomainName=<domain name>
   ```
2. To test your settings, run the following command:

   ```
   kesl-control --get-net-settings
   ```

   Trusted domains should be listed in the `[Exclusions.item_#]` section.

Example

```
kesl-control --set-net-settings Exclusions.item_0000.DomainName=example.com
```

How to exclude mount points

To exclude files in a certain directory not only from scan, but also from interception, you need to exclude the entire mount point. Such exclusions are called *global exclusions*. The application excludes trusted local or remote directories mounted on the device from scanning and interception of file operations. For example, you can exclude mount points that contain temporary files to reduce the load on the system and make scans finish sooner.

Mount point exclusions affect the following components:

- File Threat Protection
- Anti-Cryptor
- Container Scan

Trusted mount points are also excluded from scanning by the following tasks:

- Malware Scan
- Critical Areas Scan
- Container Scan
- Removable Drives Scan

> Mount points must be specified in the same way as they are displayed in the `mount` command output.

How to specify trusted mount points in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Trusted Zone** → **Mount points**.

   This opens a window containing a list of trusted mount points.
5. Click **Add**.

   This opens the form for adding a mount point.
6. In the drop-down list of file systems, select the type of the file system on which the directories to be excluded are located: **Local**, **Mounted**, **All remote mounted**.

   Kaspersky Endpoint Security supports the Samba and NFS protocols for remote directories.

   > Mount points must be specified in the same way as they are displayed in the `mount` command output.

7. Enter the name of the file system that contains the directories to be excluded.

8. To apply the policy to computers, close the padlock icons and save your changes.

How to specify trusted mount points on the command line

1. If the directory is not a mount point, create a mount point from it by running the following command:

```
mount --bind <path to dir> <path to dir>
```

2. To keep the mount point after the server reboot, add the following line to the `/etc/fstab` file:

```
<path to dir> <path to dir> none defaults,bind 0 0
```

3. Restart Kaspersky Endpoint Security:

```
systemctl restart kesl
```

4. To add a trusted mount point, run the following command:

```
kesl-control --set-app-settings ExcludedMountPoint.item_#=<path to mount point>
```

5. Restart the application to apply global exclusions:

```
systemctl restart kesl
```

Example

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000="/tmp"
```

How to add trusted applications

The *list of trusted applications* is a list of applications for which Kaspersky Endpoint Security does not monitor file and process activity (including malicious activity) or process memory. By default, Kaspersky Endpoint Security monitors objects that are opened, executed, or saved by any application process, and controls the activity of all applications.

Trusted applications affect the following components:

- File Threat Protection
- Behavior Detection

And also exclusions from scanning for process memory.

How to specify trusted applications in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Trusted Zone** → **Trusted applications**.

   This opens a window containing a list of trusted applications.
5. Select the **Merge values when inheriting** check box if you want to create a consolidated list of trusted applications for all computers in the company. The lists of trusted applications in the parent and child policies will be merged. Applications from the parent policy are displayed in child policies only for viewing, they cannot be modified or deleted.

   > To merge the lists, inheritance of the parent policy settings must be enabled.
6. Click **Add**.

   This opens the form for adding an application.
7. Specify the path to the application or a path mask.
8. Configure the trusted application settings:

   - **Do not scan files opened by this application**. All files that are opened by the application are excluded from scans by Kaspersky Endpoint Security.
   - **Do not monitor application activity**. Kaspersky Endpoint Security does not monitor the file and network activity of a trusted application within the operating system.

     You can also configure application activity monitoring separately for the MDR and EDR (KATA) components by selecting the **Do not monitor for Managed Detection and Response and Endpoint Detection and Response** check box.
   - **Do not monitor child application activity**. Kaspersky Endpoint Security does not monitor the file and network activity of applications launched by a trusted application.
   - **Do not scan memory of specified application**. Kaspersky Endpoint Security does not scan the memory of processes spawned by a trusted application.

   > In the Web Console, the **Comment** setting is not available for Kaspersky Endpoint Security for Linux.
9. Save your changes.

How to specify trusted applications on the command line

1. To exclude the file activity of a trusted application from scanning, run the following command:

```
kesl-control --set-settings 1 ExcludedForProgram.item_#.UseExcludedForProgram=Yes
ExcludedForProgram.item_#.ProgramPath=<path to app> ExcludedForProgram.item_#.AreaDesc=<trusted app name>
[ExcludedForProgram.item_#.ApplyToDescendants=Yes]
```

2. To exclude the process activity of a trusted application from scanning, run the following command:

```
kesl-control --set-set 20 UseTrustedPrograms=Yes TrustedPrograms.item_#.UseTrustedProgram=Yes
TrustedPrograms.item_#.ProgramPath=<path to app> TrustedPrograms.item_#.ProgramDesc=<trusted app name>
[TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes] [TrustedPrograms.item_#.ApplyToDescendants=Yes]
```

3. To exclude the memory of a trusted application's processes from scanning, run the following command:

```
kesl-control --set-app-settings MemScanExcludedProgramPath.item_#=<path to app>
```

Symbols

Command options

Setting	Description
`ExcludedForProgram.item_#.UseExcludedForProgram=Yes`	Exclude file activity of a trusted application from scanning by the File Threat Protection component.
`ExcludedForProgram.item_#.ProgramPath`	Path to the trusted application with ID `#`. The File Threat Protection component does not scan the processes of the specified application. If the updatable kernel module is used for system event interception, the specified process is excluded from interception in all namespaces.
`ExcludedForProgram.item_#.AreaDesc`	Trusted application name with ID `#`.
`ExcludedForProgram.item_#.ApplyToDescendants=Yes`	Exclude child processes of a trusted application from scanning by the File Threat Protection component.
`UseTrustedPrograms=Yes`	Exclude the activity of trusted applications' processes from scanning by the Behavior Detection component.
`TrustedPrograms.item_#.UseTrustedProgram=Yes`	Exclude the activity of a trusted application with ID `#` from scanning.
`TrustedPrograms.item_#.ProgramPath`	Path to the trusted application with ID `#`. The Behavior Detection component does not scan the processes of the specified application. Kaspersky Endpoint Security supports the `*` and `?` characters when entering a mask.
`TrustedPrograms.item_#.ProgramDesc`	Trusted application name with ID `#`.
`TrustedPrograms.item_#.UseTrustedProgramForMDRAndEDR=Yes`	Exclude the activity of a trusted application from telemetry collection by the Managed Detection and Response and Endpoint Detection and Response Expert (on-premises) components.
`TrustedPrograms.item_#.ApplyToDescendants=Yes`	Exclude child processes of a trusted application from scanning by the Behavior Detection component.
`MemScanExcludedProgramPath.item_#`	Path to the trusted application with ID `#`. The application does not check the memory of the trusted application's processes.

How to add trusted devices

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

To work with trusted devices, you can grant access to an individual user, to a group of users, or to all users of the organization. For example, if your organization does not allow the use of removable drives but administrators use removable drives in their work, you can allow removable drives only for a group of administrators. To do so, add removable drives to the trusted list and configure user access permissions.

You can add trusted devices based on the following data:

- **ID**. Each device has a unique identifier (Hardware ID, or HWID). You can view the ID in the device properties by using operating system tools. Example of a device ID: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. Adding devices by ID is convenient if you want to add several specific devices.

- **By ID mask**. If you are using multiple devices with similar IDs, you can add devices to the trusted list by using masks. The `*` character replaces any set of characters. The `?` character replaces any single character. For example, `WDC_C*`.

How to add trusted devices in the Kaspersky Security Center Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Device Control** → **Trusted devices**.

   This opens a window containing a list of trusted devices.

5. Click **Add**.

   This opens the form for adding a device.

6. Under **User or group**, specify a user or group of users for which the device will be considered trusted.

   You can select users in the list of accounts in Kaspersky Security Center, or by entering a local user name manually. Kaspersky recommends using local user accounts only in special cases when it is not possible to use domain user accounts.

   By default, access to trusted devices is allowed for the Everyone group.

7. Under **Device type** select a device type from the drop-down list (for example, **Removable drives**).

8. If you want to add a device based on an ID mask, select the **Use mask** check box.

9. In the **Search for trusted devices** field, enter a device ID or ID mask.

   The table displays a list of devices that satisfy the defined criteria.

10. Select the check boxes next to the names of devices that you want to add to the trusted list.

11. If necessary, describe the reason why the devices were added to the trusted list on the **Comment** tab.

12. To apply the policy to computers, close the padlock icons and save your changes.

How to add trusted devices on the command line

1. To add trusted devices, run the following command:

```
kesl-control --trusted-devices --add <device ID>
```

2. To scan the list of trusted devices of the component, run the following command:

```
kesl-control --trusted-devices --list
```

Example

```
kesl-control --trusted-devices --add WDC_C*
```

General settings

Detection settings

Detecting other types of objects

Regardless of the configured application settings, Kaspersky Endpoint Security always detects and blocks viruses, worms, and Trojans. They can cause significant harm to a computer.

You can additionally enable detection of legitimate applications that intruders can use to compromise computers or user data. Such applications do not necessarily have a malicious purpose, but can be exploited by hackers. For detailed information about legitimate applications that intruders can use to compromise the computer or user data, please visit the Kaspersky Encyclopedia website.

How to configure detection of applications that intruders can use to compromise devices or data in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

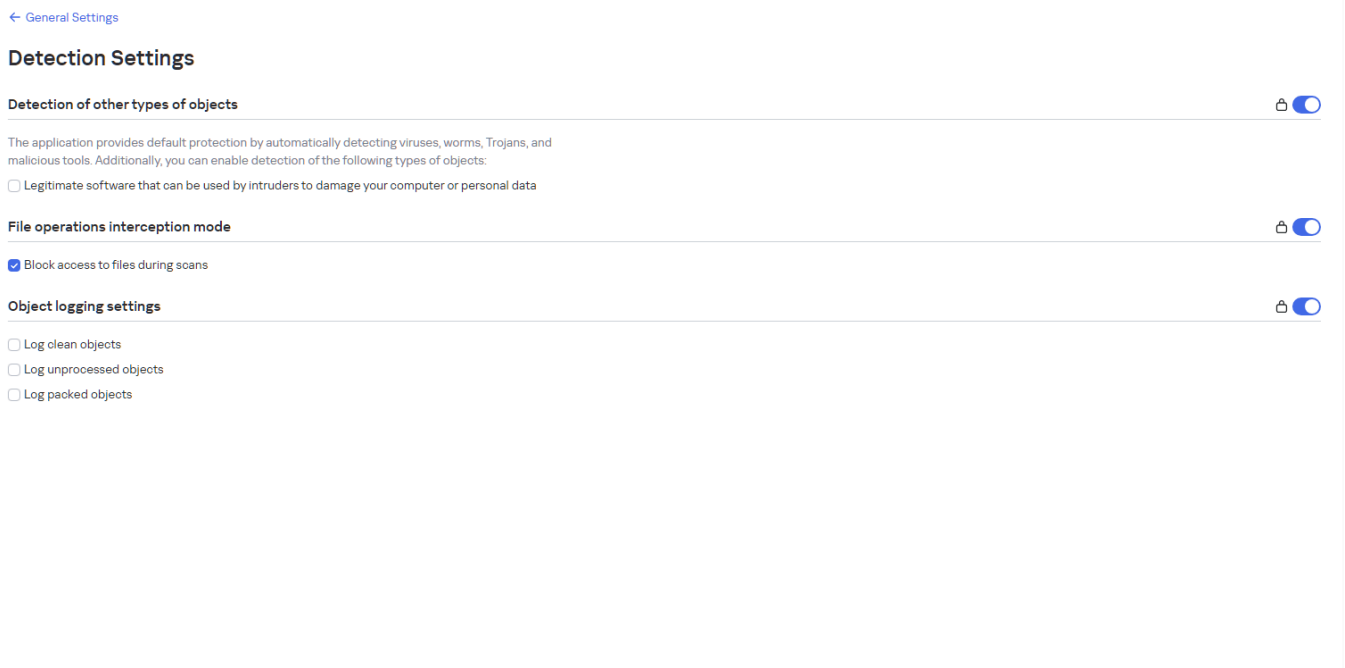
   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **General Settings** → **Detection Settings**.

5. In the **Detection of other types of objects** block, select the **Legitimate software that can be used by intruders to damage your computer or personal data** check box.

6. Save your changes.



Detection settings

How to configure detection of applications that intruders can use to compromise devices or data on the command line

1. To configure detection of applications that can be used by attackers to compromise devices or data, run the following command for application protection components:

```
kesl-control --set-app-settings DetectOtherObjects=<Yes|No>
```

2. To check links against the database of web addresses containing legitimate applications that intruders can use to compromise devices or data, run the following command in the Web Threat Protection component:

```
kesl-control --set-settings 14 CheckOther=<Yes|No>
```

3. To check the current application settings, run the following command:

```
kesl-control --get-app-settings
```

4. To check the current Web Threat Protection settings, run the following command:

```
kesl-control --get-settings 14
```

Event logging settings

By default, Kaspersky Endpoint Security does not log events about the processing of packed and uninfected objects or events about objects not processed by the File Threat Protection component.

You can enable logging for such events, making the application generate *Packed object detected*, *Object not processed*, *Object processed* events. Such events can be useful when configuring the component, as well as for debugging or troubleshooting the application. This lets you make sure that such objects have been scanned by the application and not skipped because of errors.

How to enable logging of object processing events in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Detection Settings**.
5. Under **Object logging settings**, select check boxes next to the relevant event types.
   - **Log clean objects**
   - **Log unprocessed objects**
   - **Log packed objects**
6. Save your changes.

How to enable logging of events about processing objects on the command line

1. To log events about uninfected objects, run the following command:

   ```
   kesl-control --set-settings 1 ReportCleanObjects=Yes
   ```

2. To log events about unprocessed objects, run the following command:

   ```
   kesl-control --set-settings 1 ReportUnprocessedObjects=Yes
   ```

3. To log events about packed objects, run the following command:

   ```
   kesl-control --set-settings 1 ReportPackedObjects=Yes
   ```

4. To check the current values of File Threat Protection settings, run the following command:

   ```
   kesl-control --get-settings 1
   ```

Kaspersky Security Network

To protect your computer more effectively, Kaspersky Endpoint Security uses data that is received from users around the globe. Kaspersky Security Network is designed for obtaining this data.

The KSN functionality may not be available in the application in the territory of the USA.

Kaspersky Security Network (KSN) is an infrastructure of cloud services that provides access to the Kaspersky online knowledge base, 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 Endpoint Security to new threats, improves the performance of some protection components, and reduces the likelihood of false positives. If you are participating in Kaspersky Security Network, KSN services provide Kaspersky Endpoint Security with information about the reputation of scanned web addresses, as well as information about the category and reputation of scanned files. For more details on KSN configuration, refer to the Kaspersky Security Center Help.

Use of Kaspersky Security Network is voluntary. The application prompts you to use KSN during initial configuration of the application. Users can begin or discontinue participation in KSN at any time.

Detailed information about the storage, and destruction, and/or submission to Kaspersky of statistical information generated during participation in KSN is available in the Kaspersky Security Network Statement and on Kaspersky's website. The ksn_license.<language ID> file with the text of the Kaspersky Security Network Statement is included in the application distribution package and is available in the /opt/kaspersky/kesl/doc directory.

The infrastructure of Kaspersky reputation databases

Kaspersky Endpoint Security supports the following infrastructure solutions to work with Kaspersky reputation databases:

- *Kaspersky Security Network (KSN)* is the solution that is used by most Kaspersky applications. KSN participants receive information from Kaspersky and send Kaspersky information about objects detected on the user's computer to be analyzed additionally by Kaspersky analysts and to be included in the reputation and statistical databases.

- *Kaspersky Private Security Network (KPSN)* is a solution that enables users of computers hosting Kaspersky Endpoint Security or other Kaspersky applications to obtain access to Kaspersky reputation databases, and to other statistical data without sending data to Kaspersky from their own computers. KPSN is designed for corporate customers who are unable to participate in Kaspersky Security Network for any of the following reasons:

  - Local workstations are not connected to the Internet.

  - Legal prohibition or corporate security restrictions on sending any data outside the country or the organization's local network

To use KPSN after activating application under a new license, inform the service provider about the new license key. Otherwise, an authentication error will prevent data exchange with KPSN.

Limitations of Kaspersky Private Security Network

Kaspersky Private Security Network lets you use your own local reputation database to check the reputation of objects (files or web addresses). The reputation of an object added to the local reputation database has a higher priority than one added to KSN/KPSN. For example, imagine that Kaspersky Endpoint Security is scanning a computer and requests the reputation of a file in KSN/KPSN. If the file has an *Untrusted* reputation in the local reputation database but has a *Trusted* reputation in KSN/KPSN, Kaspersky Endpoint Security will detect the file as *Untrusted* and will take the action defined for detected threats.

However, in some cases Kaspersky Endpoint Security might not request the reputation of an object in KSN/KPSN. If this is the case, Kaspersky Endpoint Security will not receive data from the local reputation database of KPSN. Kaspersky Endpoint Security might not request the reputation of an object in KSN/KPSN for the following reasons:

- Kaspersky applications are using offline reputation databases. Offline reputation databases are designed to optimize resources during operation of Kaspersky applications and to protect critically important objects on the computer. Offline reputation databases are created by Kaspersky experts based on data from Kaspersky Security Network. Kaspersky applications update offline reputation databases with anti-virus databases of the specific application. If offline reputation databases contain information about an object being scanned, the application does not request the reputation of this object from KSN/KPSN.

- Scan exclusions (trusted zone) are configured in the application settings. If this is the case, the application does not take into account the reputation of the object in the local reputation database.

- The application uses scan optimization technologies, such as iChecker or caching reputation requests to KSN / KPSN. If this is the case, the application might not request the reputation of previously scanned objects.

- To optimize its workload, the application scans files of a certain format and size. The list of relevant formats and size limits are determined by Kaspersky experts. This list is updated with the application's anti-virus databases. You can also configure scan optimization settings in the application interface, for example, for the File Threat Protection component.

- Kaspersky Endpoint Security in Light Agent mode communicates with KSN servers through a KSN proxy server. Direct communication with KSN is not supported.

How to enable or disable Kaspersky Security Network

By default, Kaspersky Endpoint Security uses the Extended KSN mode. *Extended KSN mode* is a mode in which Kaspersky Endpoint Security sends additional data to Kaspersky.

> No personal data is obtained, processed, or stored. Detailed information about the storage, and destruction, and/or submission to Kaspersky of statistical information generated during participation in KSN is available in the Kaspersky Security Network Statement and on Kaspersky's website. The file with the text of the Kaspersky Security Network Statement is included in the application distribution kit.

How to enable or disable KSN in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

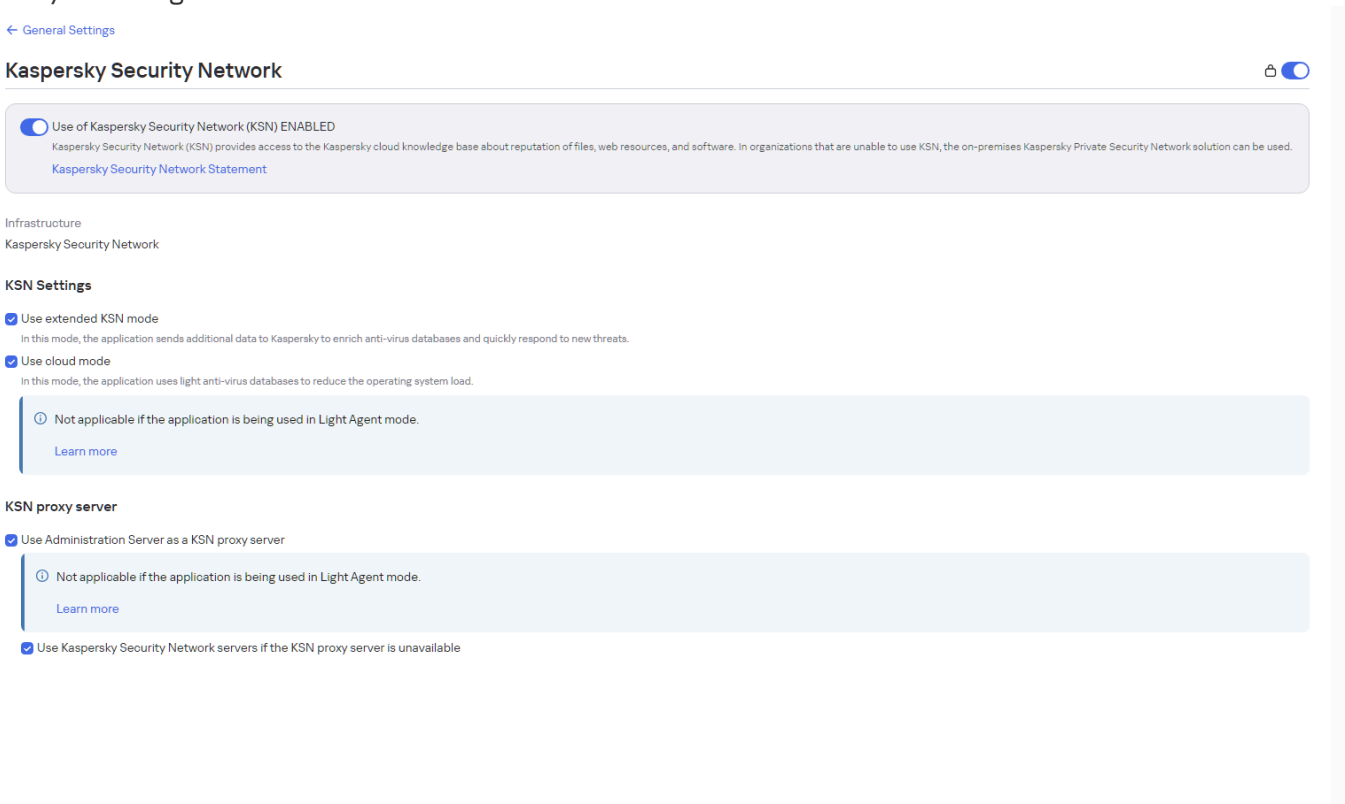
4. Go to **General Settings** → **Kaspersky Security Network**.

5. Use the **Kaspersky Security Network (KSN) usage** toggle switch to enable or disable the component.

6. If you enabled the use of KSN, the **Kaspersky Security Network Statement** window will open. Please read and accept the Kaspersky Security Network (KSN) Statement terms of use if you agree to them.

7. If required, select or clear the **Use Extended KSN mode** check box.

8. Save your changes.



Kaspersky Security Network

How to enable or disable KSN on the command line

1. Check the status of Kaspersky Security Network:

```
kesl-control --app-info
```

The application shows the status of KSN in the **Kaspersky Security Network usage** line:

- **Disabled**
- **Basic KSN mode**
- **Extended KSN mode**.

2. To enable the standard mode of Kaspersky Security Network, run the following command:

```
kesl-control --set-app-settings UseKSN=Basic --accept-ksn
```

3. To enable the extended mode of Kaspersky Security Network, run the following command:

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

4. To disable Kaspersky Security Network, run the following command:

```
kesl-control --set-app-settings UseKSN=No
```

How to enable or disable KSN Usage in the application interface

1. Open the main application window.
2. In the lower part of the main application window, click the **Settings** button.
3. In the window that opens, choose one of the following options:
   - **Extended KSN mode**, if you want to use Kaspersky Security Network, get information from the knowledge base, and send anonymous statistics and information about the types and sources of threats.
   - **Basic KSN mode**, if you want to use Kaspersky Security Network, obtain information from the knowledge base, but not to send anonymous statistics and information about the types and sources of threats.
4. Click **Enable**.
5. In the **Kaspersky Security Network usage** window, carefully read the Kaspersky Security Network Statement, and select one of the following options:
   - **I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement**.
   - **I do not accept the terms and conditions of the Kaspersky Security Network Statement**.
6. Click **OK**.

As a result, if use of KSN is enabled, Kaspersky Endpoint Security uses information about the reputation of files, web resources, and applications received from Kaspersky Security Network.

Kaspersky Endpoint Security uses the following network settings for interacting with external services:

Address	Protocol	Port
ds.kaspersky.com	HTTPS	443
ksn-a-stat-geo.kaspersky-labs.com	KSN	443, 1443
ksn-file-geo.kaspersky-labs.com	KSN	443, 1443
ksn-verdict-geo.kaspersky-labs.com	KSN	443, 1443
ksn-url-geo.kaspersky-labs.com	KSN	443, 1443
ksn-a-p2p-geo.kaspersky-labs.com	KSN	443, 1443
ksn-cinfo-geo.kaspersky-labs.com	KSN	443, 1443

What is the cloud mode of the application

In *cloud mode*, Kaspersky Endpoint Security uses a lightweight version of the anti-virus databases, which about halves the load on the RAM of the computer.

Cloud mode can be used only when Kaspersky Security Network is enabled. If you do not participate in Kaspersky Security Network or if cloud mode is disabled, Kaspersky Endpoint Security downloads the full version of anti-virus databases from Kaspersky servers. Cloud mode is enabled by default.

If the application is working in Light Agent mode, cloud mode is not available.

How to enable or disable cloud mode in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Kaspersky Security Network**.
5. Use the **Use cloud mode** toggle to enable or disable the component.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to enable or disable cloud mode on the command line

1. Run the command to display the general settings of the application to find out the current status of the application:

   ```
   kesl-control --get-app-settings
   ```

   The application shows its status in the `CloudMode` line.
2. To enable or disable cloud mode, run the following command:

   ```
   kesl-control --set-app-settings CloudMode=<Yes|No>
   ```

As a result, Kaspersky Endpoint Security downloads a light version or full version of anti-virus databases during the next update.

If the light version of anti-virus databases is not available for use, Kaspersky Endpoint Security automatically switches to the premium version of anti-virus databases.

What is the purpose of the KSN Proxy

User computers managed by Kaspersky Security Center Administration Server can interact with KSN either directly or via the KSN Proxy service.

> If the application is running in Light Agent mode, direct communication with KSN is not supported. Kaspersky Endpoint Security interacts with KSN servers using a KSN proxy server.

The KSN Proxy service provides the following capabilities:

- The user's computer can query KSN and submit information to KSN, even without direct access to the Internet.
- The KSN Proxy service caches processed data, thereby reducing the load on the external network communication channel and speeding up receipt of the information that is requested by the user's computer.

By default, after KSN is enabled and the KSN Statement is accepted, the application uses a proxy server to connect to Kaspersky Security Network. The proxy server used by the application is the Kaspersky Security Center Administration Server via TCP port 13111.

You can configure the KSN proxy server settings in the Administration Server properties. For details about the KSN proxy server, refer to the Kaspersky Security Center Help.

Configuring connection settings to the KSN proxy server using the command line is not available.

How to configure a KSN connection through a proxy server in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Kaspersky Security Network**.
5. Use the **Use Administration Server as a KSN proxy server** check box to enable or disable the use of KSN Proxy.
6. If necessary, select or clear the **Use Kaspersky Security Network servers if the KSN proxy server is unavailable** check box. This check box is selected by default.

   If this option is enabled, Kaspersky Endpoint Security uses KSN servers directly when the KSN Proxy service is unavailable. KSN servers may be located both on the side of Kaspersky and on the side of third parties (when Kaspersky Private Security Network is used).
7. Save your changes.

Configuring the transfer of data to Kaspersky Security Center storage

In Kaspersky Security Center, you can enable or disable the transfer of data about files in Backup, quarantined files, unprocessed files, and connected devices to the Kaspersky Security Center storage.

How to view quarantined files on client devices

The general list of files quarantined by Kaspersky applications on client devices is kept in Kaspersky Security Center.

1. In the main window of Web Console, select **Operations** → **Repositories**.
2. Go to the **Quarantine** folder.
3. Information about quarantined objects is displayed in the right pane of the console.

How to view files in Backup on client devices

The general list of files placed in Backup by Kaspersky applications on client devices is kept in Kaspersky Security Center.

1. In the main window of Web Console, select **Operations** → **Repositories**.
2. Go to the **File backups** folder.
3. Information about objects placed in Backup is displayed in the right pane of the console.

How to view information about unprocessed files in the list of active threats

1. In the main window of Web Console, select **Operations** → **Repositories**.
2. Go to the **Active threats** folder.
3. Information about unprocessed files in the list of active threats is displayed in the right pane of the Console.

How to view information about hardware connected to client devices

1. In the main window of Web Console, select **Operations** → **Repositories**.
2. Go to the **Hardware** folder.
3. Information about devices is displayed in the right pane of the Console.

Data is transferred if Device Control is enabled.

How to view information about applications on client devices

1. In the main window of Web Console, select **Operations** → **Third-party applications**.
2. Go to the **Applications registry** folder.
3. Information about applications is displayed in the right pane of the Console.

Data is transferred if Application Control is enabled.

How to configure integration with the Administration Server

To configure the Administration Server integration in the policy properties:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **KSC Integration**.
5. Click the **Additional settings** link.

6. Select categories of events on client computers whose information must be relayed to the Administration Server:

   - **About files in Quarantine** This check box enables or disables the transfer of data about quarantined files to the Administration Server.

   - **About files in Backup**. This check box enables or disables the transfer of data about files in Backup to the Administration Server.

   - **About unprocessed files**. This check box enables or disables sending notifications about the files, which were not processed during the scan, to the Administration Server.

   - **About installed devices**. This check box enables or disables the transfer of data about devices installed on a client device or connected to it, to the Administration Server.

   - **About started applications**. This check box enables or disables the sending of the list of applications that the Inventory task discovers on the client device to the Administration Server.

7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

To configure the Administration Server integration in the properties of a managed device:

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)** → **Managed devices**.

2. Click the **<device name>** link.

3. Select the **Applications** tab and click the **Kaspersky Endpoint Security** link.

4. On the **Application settings** tab, go to the **Storage settings** section.

5. Under **Settings for transferring data to the Administration Server**, click the **Configure** button.

6. In the **Data transfer settings** window, you can enable or disable sending information to the Administration Server:

   - **Notify about files in Backup**. This check box enables or disables the transfer of data about files in Backup to the Administration Server.

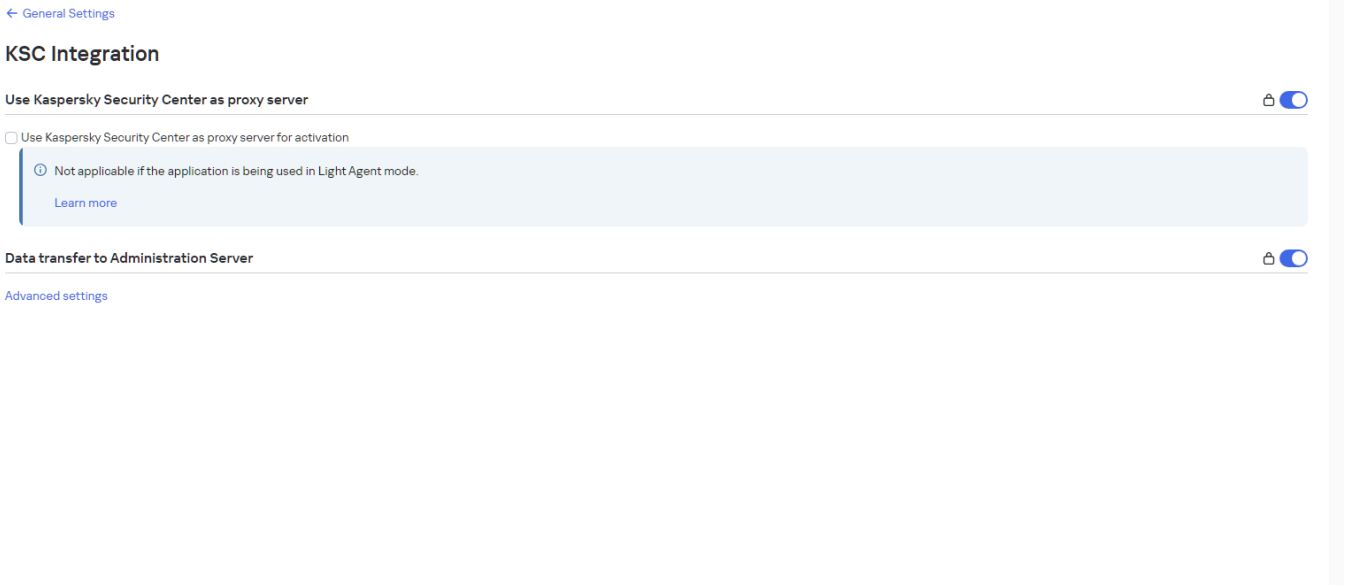
   - **Notify about files in Quarantine**. This check box enables or disables the transfer of data about quarantined files to the Administration Server.

   - **Notify about unprocessed files**. This check box enables or disables sending notifications about the files, which were not processed during the scan, to the Administration Server.

   - **Notify about installed devices**. This check box enables or disables the transfer of data about devices installed on a client device or connected to it, to the Administration Server.

   - **Notify about applications found on the device**. This check box enables or disables the sending of the list of applications that the Inventory task discovers on the client device to the Administration Server.

7. Save your changes.



Integration with Kaspersky Security Center

How to configure application startup

Configuring application startup

You can configure the maximum number of unsuccessful launch attempts and the launch timeout for Kaspersky Endpoint Security. This allows reducing the load on the system if the application cannot start for a long time. By default, the maximum number of unsuccessful successive attempts to launch the application in a row is 5, the maximum timeout is 3 minutes.

How to configure application startup in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **User Interaction**.
5. Under **Application startup settings**, enter values in the following fields:
   - **Maximum consecutive unsuccessful attempts to start the application**. Default value: 5.
   - **Maximum time to wait for application start (min)**. Default value: 3.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to configure application startup on the command line

In the command line, you can configure application startup settings using the `MaxRestartCount` and `StartupTimeout` settings in the kesl.ini configuration file.

The `MaxRestartCount` setting lets you set the maximum number of unsuccessful consecutive attempts to start the application. The setting can take values from 1 to 10. Default value: 5.

The `StartupTimeout` setting lets you set the maximum time to wait for the application to start (in minutes), after which the kesl process will be restarted. The setting can take values from 1 to 60. Default value: 3.

Applying critical updates

You can configure the application to automatically restart when receiving critical updates after the first 24 hours after installing the application. During the first 24 hours after installation, the application automatically restarts when critical updates are received, without additional configuration.

How to configure the automatic application restart in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **User Interaction**.
5. In the **Applying critical updates** block, select the **Automatically restart the application when critical updates are received** check box.

   The Kaspersky Endpoint Security application will restart when it receives critical updates one day after the application is installed.
6. Save your changes.

How to configure the automatic application restart on the command line

You can configure automatic application restart on the command line using the `UrgentUpdateRestartEnabled` setting in the general application settings.

To automatically restart the application when installing critical updates, run the following command:

```
kesl-control --set-app-settings UrgentUpdateRestartEnabled=Yes
```

Configuring permissions for task management

You can define the following user permissions in Kaspersky Security Center:

- Using local tasks created in Kaspersky Endpoint Security. If the Kaspersky Security Center policy prevents users from viewing, editing, creating, and deleting local tasks, information about the Scan_My_Computer, Critical_Areas_Scan, Container_Scan, Inventory_Scan, Update (in Standard mode) and Rollback (in Standard mode) tasks is not available.

- Viewing and managing tasks created in Kaspersky Security Center on client devices.

To configure task management permissions in the Web Console:

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **General Settings** → **User Interaction**.

5. Under **Permitted actions**, select the actions that users are allowed to perform on their devices:

   - **Access to local tasks**. If the check box is selected, local tasks are displayed in the Kaspersky Endpoint Security local interface. If further policy restrictions do not prevent this, users can configure, run, create, and delete available local tasks in the graphical interface of the application or on the command line.

   - **Manage group tasks**. If this checkbox is selected, users can manage group tasks configured in Kaspersky Security Center on client devices. Tasks can be run from the graphical interface of the application or the command line.

6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

Password protection

Password protection allows you to restrict user access to modifying Kaspersky Endpoint Security in accordance with the permissions granted (for example, permission to view application reports). Restricting access to application settings reduces the risk of unauthorized or unintentional changes to the application.

How Password protection works

1. **A user tries to perform an action controlled by the component**

   For example, disabling protection components or viewing Kaspersky Endpoint Security reports.

2. **Kaspersky Endpoint Security checks user rights**

   If the user has the corresponding permission, the action is performed successfully. If the user does not have the corresponding permission, the application blocks the action and displays an error.

   In the graphical interface of Kaspersky Endpoint Security, prohibited actions cannot be viewed or edited.

Configuring Password protection

1. **Enable Password protection**

   By default, Password protection is disabled. Enable the component in the Web Console or the Administration Console, or on the command line using the following command:

   ```
   kesl-control --set-permission-manager-settings Enabled=Yes
   ```

2. **Configure user permissions**

   By default, the application has user permissions configured for predefined user groups: *kesladmin*, *kesluser*, *keslaudit*.

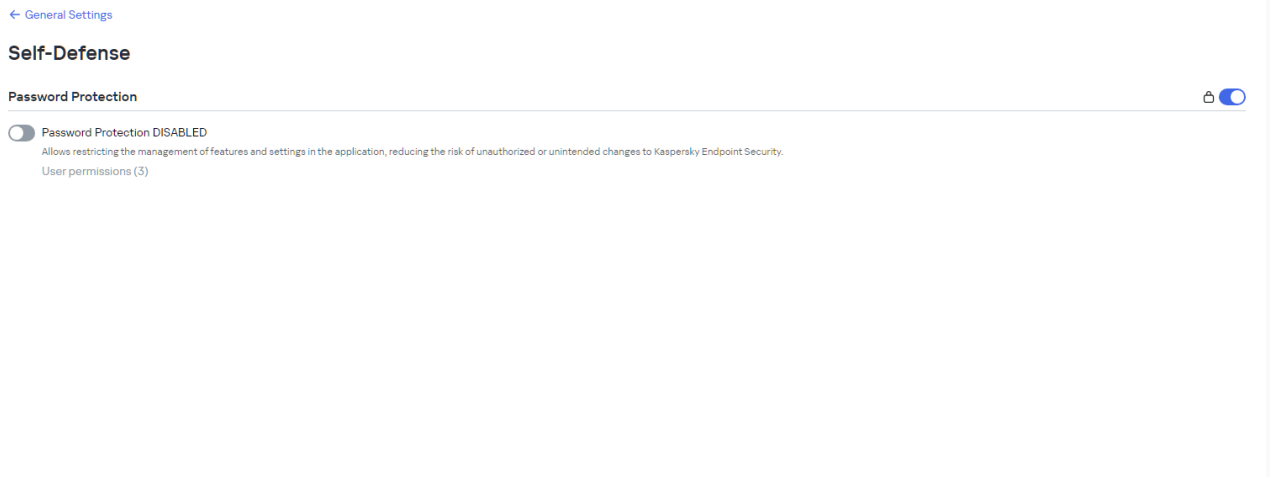
   Configure user permissions for these groups, or create a new user or user group.

   > For the application to work correctly, we recommend configuring permissions for at least one group.

   How to configure custom permissions in the Web Console

   1. In the main window of the Web Console, select **Asset management** → **Policies**.
   2. Click the name of the Kaspersky Endpoint Security policy.
      The policy properties window opens.
   3. Select the **Application settings** tab.
   4. Go to **General Settings** → **Self-Defense**.
   5. Make sure the toggle switch for the component is in the **Password Protection ENABLED** position.
   6. Click the **User permissions** link.
      This opens a window with users and their permissions.
   7. If you want to change permissions for predefined groups, click a group's name.
      If you want to change permissions for another user or group:
      a. Click **Add**.
      b. Select a user or group from Active Directory or enter the name manually.
   8. Select the check boxes next to the permissions that you want to grant to the user or group.

9. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Self-Defense

How to configure custom permissions on the command line

1. To view the list of current Password protection settings, run the following command:

```
kesl-control --get-permission-manager-settings
```

2. To change the permissions of a user or group, run the following command:

```
kesl-control --set-permissions <principal> [--group] <permissions>=<Yes|No> [--file <file name>] [--
json]
```

3. To remove a user or group for which permissions have been configured, run the following command:

```
kesl-control --remove-permissions <principal> [--group]
```

Symbols

Command options

Setting	Description
`--group`	The setting applies to a group. If the `--group` option is not specified, the setting applies to an individual user.
`--file <file name>`	Outputting parameters to a file or importing parameters from a file. Enter a `<file name>`.
`--json`	Outputting parameters to a JSON file or importing parameters from a JSON file. This option can be specified only if the `--file <file name>` option is specified.
`principal`	User or user group name.
`permissions`	Custom permissions. Specify `Yes` to allow an action to the user, or `No` to deny. • `StopProtection`. Disabling protection components. • `StopSecurityControl`. Disabling control components • `StartProtection`. Enabling protection components. • `StartSecurityControl`. Enabling control components • `ApplicationSettings`. Configuring the application • `ViewReports`. Viewing reports • `RestoreFromBackup`. Restoring from Backup • `RemoveLicenseKey`. Remove key • `AddLicense`. Adding a key • `DisablePolicy`. Disabling the Kaspersky Security Center policy

Examples

Revoke permission to view reports from the *kesluser* group:

```
kesl-control --set-permissions kesluser --group ViewReports=No
```

Allow management of control components to *new-user*:

```
kesl-control --set-permissions new-user startSecurityControl=Yes StopSecurityControl=Yes
```

Special considerations for Password protection

- If Password protection is disabled, whether a user is allowed to manage the application is determined by user roles.
- If a user's access level is governed by group permissions as well as individual permissions, individual permissions override group permissions. That is, even if a user's individual permissions are more restrictive than the same user's group permissions, the more restrictive permissions prevail.

  For example, if managing the application is forbidden to the *kesluser* group, you can still allow managing the application to an individual user that is a member of this group. Such a user is still allowed to manage the application even though group permissions do not allow it.
- If Password protection is enabled and a user has neither individual nor group permissions, all actions are forbidden.

About custom permissions

If Password protection is enabled, access to managing Kaspersky Endpoint Security is controlled using *user permissions*. User permissions define the rights of a user (see the table below).

Custom permissions

Permission	Permissions
Configuring the application	Viewing and editing application settings. Managing task settings in the graphical interface of the application and on the command line without using the `sudo` command. Assigning roles to users. Revoking user roles (the administrator has no right to revoke the admin role from himself). Managing the *Rollback* task. Managing components: • Managed Detection and Response • Endpoint Detection and Response Optimum

Permission	Permissions
Enabling protection components.	Managing components: • File Threat Protection • Removable drives scan • Behavior Detection • Anti-Cryptor • BadUSB Attack Prevention • Mail Threat Protection • Web Threat Protection • Network Threat Protection • Firewall Management • System Integrity Monitoring • Execution prevention for objects (EDR Optimum) (*EDRO_Prevention*) • Endpoint Detection and Response Expert (on-premises) • Endpoint Detection and Response Expert (cloud) • Network Detection and Response (KATA) • Sandbox • Integration with KUMA
Disabling protection components	
Enabling control components	Managing components: • Device Control • Application Control • Web Control
Disabling control components	
Viewing reports	Viewing task reports Viewing events
Restoring from Backup	View and manage users' Storages.
Deleting the key	Manage application licensing.
Add a key	
Disabling the Kaspersky Security Center policy	Disabling or enabling the Kaspersky Security Center policy on the device.

Special considerations involved with custom permissions

- User permissions do not affect viewing the list of tasks, viewing objects in Backup, viewing the settings and status of the application.

  All users are allowed to manage the following tasks:

  - Scan tasks (*Custom Scan*, *Container Scan*, *Custom Container Scan*, *Critical Areas Scan*, *Malware Scan*)
  - *Inventory*
  - *Update of databases and application modules*
  - *System Integrity Check*
  - *IOC search*

- You cannot adding or remove the main license key in the graphical interface if the device is controlled by a Kaspersky Security Center policy. A user with *Add key* and *Remove key* permissions may add a reserve key or a license key for activating other Kaspersky solutions (add-on).

  If the device is not managed by a policy, the user can remove or add the main license key.

Default user permissions

By default, the application has user permissions configured for predefined user groups: *kesladmin*, *kesluser*, *keslaudit*. For users that are not members of these groups, all operations with the application are forbidden.

User permissions of predefined groups

Permission	kesladmin	kesluser	keslaudit
Configuring the application	✓	–	–
Enabling protection components.	✓	–	–
Disabling protection components	✓	–	–
Enabling control components	✓	–	–
Disabling control components	✓	–	–
Viewing reports	✓	–	✓
Restoring from Backup	✓	–	–
Deleting the key	✓	–	–
Add a key	✓	–	–
Disabling the Kaspersky Security Center policy	✓	–	–

Performance settings

Scanning the computer using the Kaspersky Endpoint Security application may utilize significant system resources. To optimize the load on the system, you can:

- Postpone or skip scheduled tasks while running on battery power
- Limit CPU usage by scan tasks (%)
- Limit resident memory usage by the application
- Exclude memory of some processes from scanning

Postpone or skip scheduled tasks while running on battery power

If your device is running on battery power and you want to reduce resource usage by Kaspersky Endpoint Security, you can skip scheduled tasks:

- All scan tasks (Custom Scan, Container Scan, Custom Container Scan, Critical Areas Scan, *Malware Scan*)
- *Inventory*
- *Update of databases and application modules*
- *Application Integrity Check*
- *IOC Scan*

You can run tasks manually as needed.

How to cancel scheduled tasks when running on battery power using the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Performance**.
5. Enable the **Postpone or skip scheduled tasks while running on battery power** functionality.
   Kaspersky Endpoint Security *cancels* scheduled tasks.
6. Save your changes.

How to cancel scheduled tasks when running on battery power using the command line

You can configure the cancellation of scheduled tasks on the command line using the `PowerSaveMode` setting in the general application settings.

To cancel scheduled tasks when the device runs on battery power, run the following command:

```
kesl-control --set-app-settings PowerSaveMode=Yes
```

Limit CPU usage by scan tasks (%)

You can limit the CPU and memory usage for the *Malware Scan*, *Critical Areas Scan*, *Inventory*, and *Container Scan* tasks (of the ODS, ContainerScan, and InventoryScan types). By default, the memory usage limit is set to 8192 MB. No limit is set for CPU usage.

> It is recommended that you set the memory usage limit for scan tasks below the resident memory usage limit so that scan tasks do not consume all available RAM and cause the application to restart.

> Note that the combined capacity of all CPU cores is considered to be 100%.

In the output of the `top` utility, 100% corresponds to the full utilization of a single core. Thus, for a 10-core CPU (reported by the `top` utility as 1000% total), a value of 400% means that the usage of the entire CPU (all cores taken together) is 40%. If you want the value in the output of the `top` utility to never exceed 150% on the same 10 cores, set a CPU usage limit of `15%`.

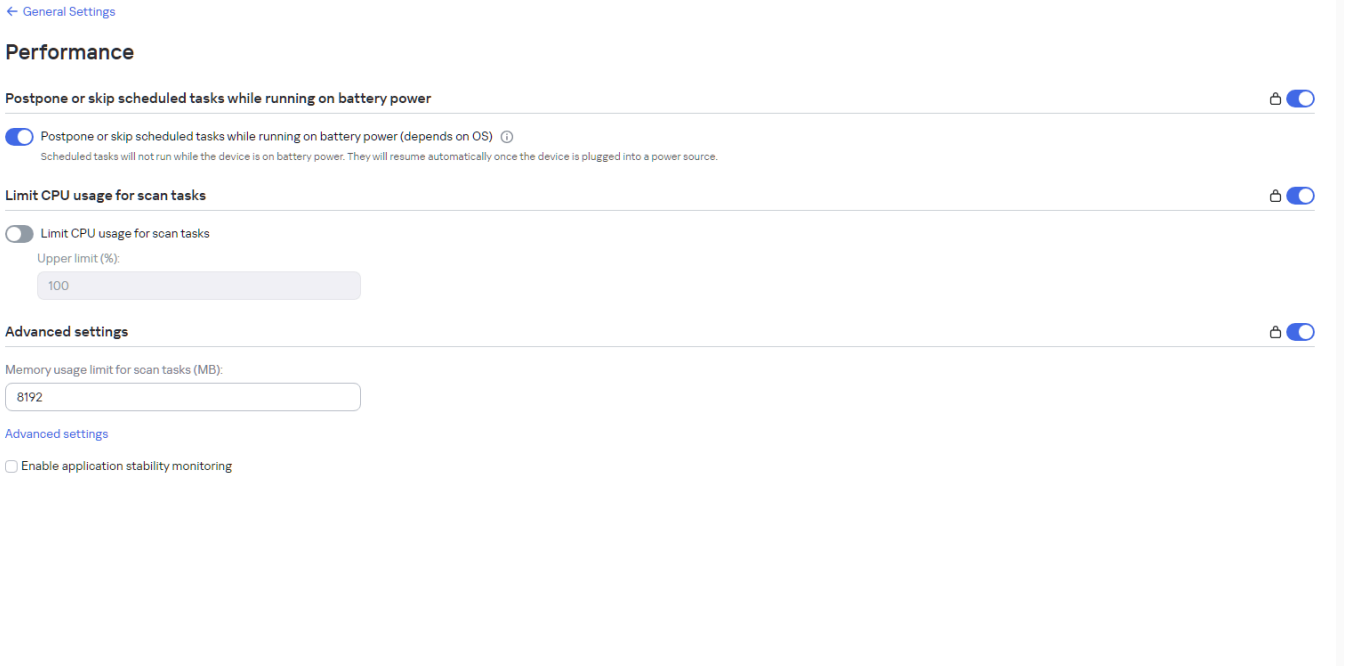
The CPU usage limit is applied to the *Malware Scan*, *Critical Areas Scan*, *Inventory*, and *Container Scan* tasks, which means that the CPU usage may exceed the configured value.

> Limiting CPU usage is not possible on devices running CentOS 5.2 and 5.4.

How to limit memory and CPU resource usage in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Performance**.
5. Enable the **Limit CPU usage for scan tasks** functionality.
6. Specify the maximum load on all CPU cores in the **Upper limit (%)** field. The value must be an integer from 10 to 100.
7. Under **Advanced settings**, specify the memory usage limit for scan tasks (MB) in the corresponding field. Default value: 8192.
8. To apply the policy to computers, close the padlock icons and save your changes.



Performance

How to limit memory and CPU resource usage on the command line

On the command line, you can configure a limit on CPU resource usage for scan tasks using the `UseOnDemandCPULimit` and `OnDemandCPULimit` settings in the general application settings.

1. Enable the CPU limit for scan tasks by running the following command:

```
kesl-control --set-app-settings UseOnDemandCPULimit = Yes
```

2. Set a CPU limit by running the following command:

```
kesl-control --set-app-settings OnDemandCPULimit =<value>
```

   The limit is set as a percentage; possible values are integers from 10 to 100.

3. Specify the memory usage limit for scan tasks by managing the `ScanMemoryLimit` setting in the kesl.ini configuration file.

Limit resident memory usage by the application

You can limit resident memory usage by the application. By default, the limit is set up to 50% of memory, but not less than 2 GB and not more than 16 GB.

How to limit resident memory usage in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Performance**.
5. Under **Advanced settings**, click the **Advanced settings** link and in the displayed window, select the **Limit application memory usage** check box.

   In the drop-down list, you can select how to limit resident memory usage:

   - **Set an exact value (%)**. When this item is selected, the **Exact value (%)** field becomes available, in which you can specify a percentage value. The default value is 50%
   - **Set an exact value (MB)**. When this item is selected, the **Exact value (MB)** field becomes available, in which you can specify a value in megabytes. The default value is 2000 MB.
   - **Use the highest of the two values (% or MB)**. When this item is selected, the **Exact value (%)** and **Exact value (MB)** fields become available, in which you can specify the necessary values.
   - **Use the lowest of the two values (% or MB)**. When this item is selected, the **Exact value (%)** and **Exact value (MB)** fields become available, in which you can specify the necessary values.
   - **Limit automatically (recommended)**. When this item is selected, resident memory usage is limited automatically (default value).
6. Save your changes.

To apply the changes, restart the Kaspersky Endpoint Security application on the managed device after the policy has been applied.

How to limit resident memory usage on the command line

You cannot manage the `MaxMemory` setting on the command line. Use the kesl.ini configuration file to configure the resident memory limit.

> Changing the default values is only recommended under the supervision of the Technical Support specialists and based on their instructions.

The `MaxMemory` parameter can take the following values:

- `off` – the resident set size is not limited.
- `<value>%` – a value between 1 and 100 percent of RAM.
- `<value>MB` – a value in megabytes.
- `lowest/<value>%/<value>MB` – the smaller of the percentage value and the absolute value in megabytes.
- `highest/<value>%/<value>MB` – the larger of the percentage value and the absolute value in megabytes.
- `auto` (default) – automatic limit.

Excluding process memory from scans

You can exclude the memory of selected processes from scanning.

How to exclude process memory from scanning in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Performance**.
5. In the **Advanced settings** block, click the **Configure exclusion of process memory from scans** link.
6. This opens a window; in that window, click the **Add** button and specify the path to the executable file of the process.
   Path requirements:
7. Must start with `/` (absolute path)
   a. Must not contain forbidden characters:
      - `\0` (null byte): prohibited by the operating system.
      - Slash (`/`) inside a file or directory name: used as a separator.
8. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to exclude process memory from scanning on the command line

You can configure excluding process memory from scans in the command line using the `MemScanExcludedProgramPath.item_#` option in the general application settings.

You can change the value of the setting with the help of command line switches or a configuration file that contains all general application settings.

`MemScanExcludedProgramPath.item_#` contains the full path to the process in the local directory. You can use masks to specify the path.

You can specify several processes to exclude from scanning.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Optimizing resource consumption by the application

Network settings

You can configure the proxy server used for connecting to the internet, select the network port monitoring mode, and set up an encrypted connections scan.

How to manage proxy settings

You can configure proxy server settings if the users of the client devices use a proxy server to connect to the internet. The Kaspersky Endpoint Security application can use a proxy server to connect to Kaspersky activation servers, to update sources for databases and application modules, to Kaspersky Security Network, and when verifying website certificates using the Web Threat Protection component.

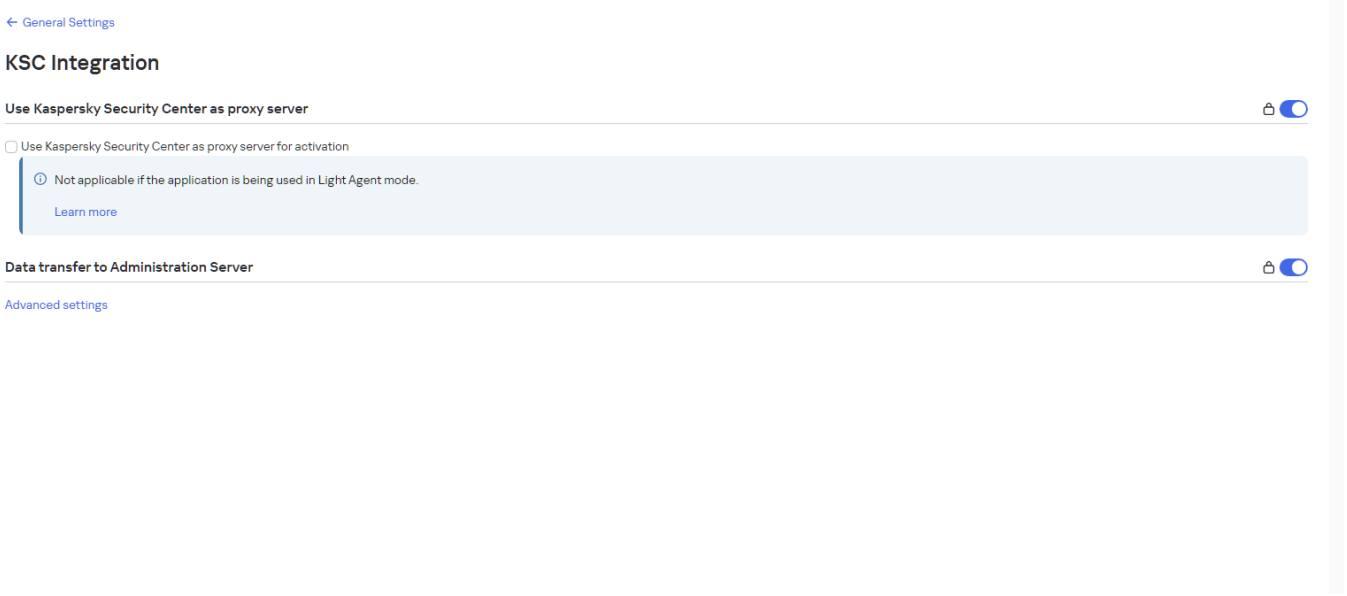
The proxy server is not used by default.

If you use an activation code to activate devices in an isolated network segment without internet access, you can use Kaspersky Security Center Administration Server as a proxy server for access to Kaspersky activation servers.

How to configure the use of Kaspersky Security Center as a proxy server for activating the application in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **General settings** → **KSC Integration** section.
5. Select the **Use Kaspersky Security Center as a proxy server for activation** check box.
6. Click the **Save** button.



Integration with Kaspersky Security Center

If Kaspersky Endpoint Security is used in Light Agent mode, the use of a proxy server for connecting to Kaspersky Security Network, the SVM, and the Integration Server is not supported. Also, using the Administration Server as a proxy server for access to Kaspersky activation servers is not supported in Light Agent mode.

How to manage proxy settings in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Network Settings**.
5. Set the toggle switch to **Use of proxy server ENABLED**.
6. In the displayed window, fill in the fields:
   - **Proxy server address**.
   - **Proxy server port**.

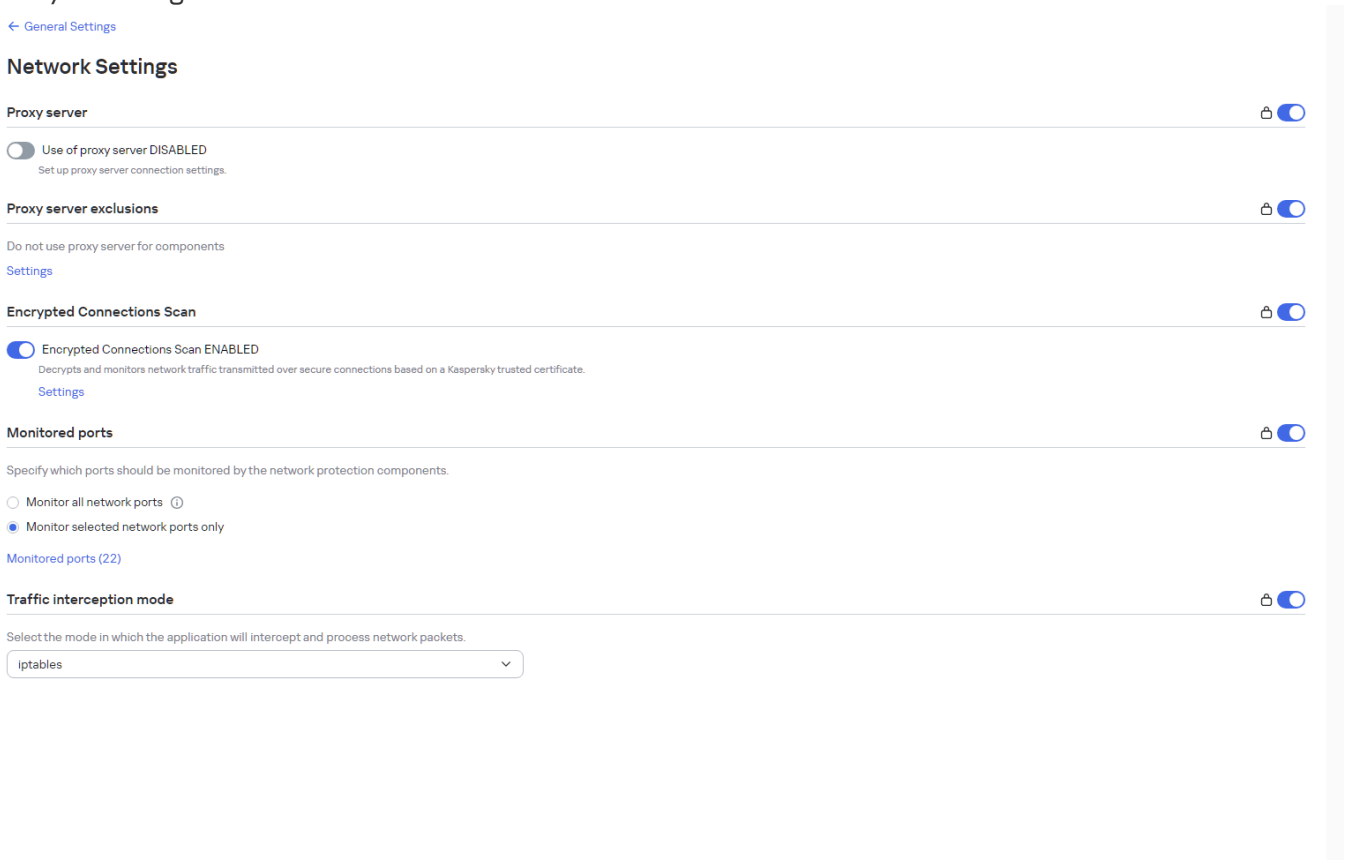
7. If necessary, enable proxy server authentication:

   a. Select the **Use proxy server authentication** check box.

   b. Fill in the fields:

   - **User name**.
   - **Password**.

8. Save your changes.



Network settings

How to manage proxy settings on the command line

1. To enable the use of a proxy server, run the following command:

```
kesl-control --set-net-settings UseProxy=Yes ProxyServer=<proxy server address>
```

2. To check the current values of network settings, run the following command:

```
kesl-control --get-net-settings
```

Symbols

Command options

Setting	Description
`ProxyServer`	Address of the proxy server used to connect to the Internet. Address of the proxy server in one of the following formats: • `[<connection protocol>://]<address of the proxy server>:<port>`, if no authentication is required to connect to the proxy server; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, if authentication is required when connecting to the proxy server. When specifying an IPv6 address, enter it in square brackets. Connecting to a proxy server over HTTPS is not supported. When connecting via an HTTP proxy, we recommend to use a separate account that is not used to sign in to other systems. An HTTP proxy uses an insecure connection, and the account may be compromised.

Proxy server exclusions

If you do not need to use a proxy server for connections to some addresses, you can add such addresses to exclusions.

You can also disable the use of a proxy server for the EDR Expert (on-premises), NDR (KATA), and Sandbox components, which provide integration with Detection and Response solutions. When connecting to these components' integration servers, the proxy server will not be used.

How to configure proxy server exclusions in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Network Settings**.
5. In the **Proxy server exclusions** block, click the **Settings** link.

   This opens a proxy server exclusions window
6. Select the check boxes for the components with which you do not want to use a proxy server:
   - **Endpoint Detection and Response Expert (on-premises)**
   - **KATA Sandbox**.
   - **Network Detection and Response (KATA)**.
7. Add IP addresses for which you do not want to use a proxy server. Example: `1.2.3.4/24`, `1234::cdef/96`.
8. Save your changes.

How to configure proxy server exclusions on the command line

1. To add addresses for which you do not want to use a proxy server, run the following command:

```
kesl-control --set-net-settings ProxyBypass=<address:port>
```

2. To bypass the proxy server for integrations with Kaspersky Detection and Response solutions, run the following command:

```
kesl-control --set-net-settings [ProxyBypassEdr=<Yes|No>] [ProxyBypassNdr=<Yes|No>] [ProxyBypassSandbox=
<Yes|No>]
```

3. To check the current values of network settings, run the following command:

```
kesl-control --get-net-settings
```

Symbols

Command options

Setting	Description
`ProxyBypass`	List of addresses for which the proxy server is to be bypassed. The address is specified in the `<address>[:<port>]` format. To specify addresses, you can use masks (`*` symbol) and comments after a `\` symbol.
`ProxyBypassEdr`	Whether a proxy server is used when connecting to Kaspersky Endpoint Detection and Response Expert (on-premises) integration servers. The proxy server is not used by default (`No`).
`ProxyBypassNdr`	Whether a proxy server is used when connecting to Kaspersky Network Detection and Response (KATA) integration servers. The proxy server is not used by default (`No`).
`ProxyBypassSandbox`	Whether a proxy server is used when connecting to servers that provide interaction with Sandbox. The proxy server is not used by default (`No`).

How the application intercepts traffic

An application can work in one of two network traffic interception modes: eBPF or iptables. The iptables mode is selected by default.

This setting is not applicable to devices with an Elbrus CPU.

About eBPF network traffic interception

In the eBPF mode, the application creates its own separate network namespace (network linux namespace), where it redirects network packets using eBPF programs associated with `tc` (linux traffic control) queues of local network interfaces. The redirected network traffic is then analyzed in accordance with active network tasks and then is returned to the original network interface.

For communication between namespaces, pairs of `veth` virtual network interfaces are used (each side of a pair is in its own network namespace):

- The `kesl_in - kesl_worm_in` pair transmits network traffic of inbound connections.
- The `kesl_out - kesl_worm_out` pair transmits network traffic of outbound connections.

Through these pairs of interfaces, network traffic is sent for scanning from the default namespace to the namespace created by the application, and through the same interfaces, the traffic is returned back after analysis.

Network traffic reaches these interfaces from other network interfaces in the system only if the application is running and network interception is enabled. These interfaces cannot be used for data transmission over the network between remote devices.

About iptables network traffic interception

In iptables mode, interception is performed using the tproxy kernel mechanism.

Corresponding rules are created in the PREROUTING chain of the mangle table that forward traffic to a special port opened by the application. The application also adds extra rules to various tables of the operating system's firewall to forward packets to tproxy. The application's network interceptor sits between the client and the server and establishes a separate connection with each of them, and scans and transmits traffic between them.

Intercepted inbound and outbound connections are marked with separate labels, which you can change in the kesl.ini configuration file.

For outbound connections, additional routing rules are introduced that redirect outbound traffic for intercepted ports to the loopback interface in tproxy.

Selecting traffic interception mode

How to select a network traffic interception mode in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Network Settings**.
5. Under **Traffic interception mode**, select a traffic interception mode for the application:
   - **iptables**. Selected by default. The application uses the iptables tool to intercept traffic.
   - **eBPF**. The application uses the eBPF technology to intercept traffic.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to select a network traffic interception mode on the command line

1. Run the following command:

```
kesl-control --set-net-settings NetInterceptorMode=<UseEBPF|UseIPTables>
```

2. To check the current values of network settings, run the following command:

```
kesl-control --get-net-setting
```

Special considerations and limitations

- To change the traffic interception mode, you need to restart the application. Restarting breaks established network connections.
- If the application is unable to use eBPF mode to intercept network traffic, iptables mode will be used instead.

How to configure certificate validation policy

Network traffic scanning settings are used by Web Threat Protection, Network Threat Protection, Mail Threat Protection, and Web Control.

By default, Web Threat Protection decrypts and scans network traffic sent over encrypted connections. To achieve this, the application validates the entire certificate chain.

The certificate validation policy includes the following settings:

- Validation method (locally or via the internet)
- Access to websites with an untrusted certificate
- Access to websites with a certificate validation error

If the device does not have a direct internet connection, you can select the local certificate validation method.

By default, the application allows establishing a network connection to a domain with an untrusted certificate. The application displays an HTML page with a warning and information about the reason why it is not recommended to visit the relevant domain (see the figure below). A user can click the link from the HTML warning page to obtain access to the requested web resource.

If a third-party application or service establishes a connection with a domain with an untrusted certificate, the application creates its own certificate to scan traffic. The new certificate has the *Untrusted* status. This is necessary to warn the third-party application about the untrusted connection because the HTML page cannot be shown in this case and the connection can be established in background mode.

Certificate validation may end with an error. For example, when working with cloud storage or when validating self-signed certificates. By default, the application adds domain names of such websites to exclusions and does not control encrypted network traffic when this domain is visited. The application also generates an event for the encrypted connection scan error.

> You can view a list of domains with encrypted connections scan errors only in the local interface of the application.

How to configure the certificate validation policy in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Network Settings**.
5. Under **Encrypted Connections Scan**, make sure the toggle switch is in the **Encrypted Connections Scan ENABLED** position.

   If the toggle switch is disabled, Kaspersky Endpoint Security does not have access to the content of websites whose addresses begin with `https://`.
6. Follow the **Settings** link and configure the certificate validation policy:
   - **Visiting a domain with an untrusted certificate**. Action when an untrusted certificate is encountered
     - **Allow connection**. The application allows connections to a domain with an untrusted certificate. The application displays an HTML page with a warning and information about the reason why it is not recommended to visit the relevant domain (see the figure below). A user can click the link from the HTML warning page to obtain access to the requested web resource.
     - **Block connection**. When visiting a domain with an untrusted certificate, Kaspersky Endpoint Security blocks the network connection and displays an HTML page showing the reason why that domain is blocked.
   - **Visiting a domain with an encrypted connections scan error**. Action on an encrypted connection scan error:
     - **Allow and add domain to exclusions**. When an encrypted connection scan error occurs, the application adds the domain that resulted in the error to the list of exclusions and does not monitor encrypted network traffic when this domain is visited.
     - **Block connection**. When an encrypted connection scan error occurs, Kaspersky Endpoint Security blocks the network connection.

- **Certificate verification policy**. How the application validates certificates:
  - **Full check**. The application uses the internet to check and download the missing chains that are needed to validate a certificate.
  - **Local check**. The application validates the certificate locally on the computer.

7. To apply the policy to computers, close the padlock icons and save your changes.

How to configure a certificate validation policy on the command line

1. To enable encrypted connection scanning, run the following command:

```
kesl-control --set-net-settings EncryptedConnectionsScan=Yes
```

2. To select a certificate validation method, run the following command:

```
kesl-control --set-net-settings CertificateVerificationPolicy=<FullCheck|LocalCheck>
```

3. To select an action to take when an untrusted certificate is found, run the following command:

```
kesl-control --set-net-settings UntrustedCertificateAction=<Allow|Block>
```

4. To select an action to take when an error occurs during an encrypted connection scan, run the following command:

```
kesl-control --set-net-setting EncryptedConnectionsScanErrorAction=<AddToAutoExclusions|Disconnect>
```

5. To check the current values of network settings, run the following command:

```
kesl-control --get-net-setting
```

Symbols

Command options

Setting	Description
`EncryptedConnectionsScan`	Encrypted connections scan mode: `Yes` (default). Encrypted connections scan is enabled. `No`. Encrypted connections scan is disabled.
`CertificateVerificationPolicy`	Certificate validation policy: `FullCheck` (default). The application uses the internet to check and download the missing chains that are needed to validate a certificate. `LocalCheck`. The application validates the certificate locally on the computer.
`UntrustedCertificateAction`	Action when an untrusted certificate is encountered `Allow` (default). The application allows connections to a domain with an untrusted certificate. The application displays an HTML page with a warning and information about the reason why it is not recommended to visit the relevant domain (see the figure below). A user can click the link from the HTML warning page to obtain access to the requested web resource. `Block`. When visiting a domain with an untrusted certificate, Kaspersky Endpoint Security blocks the network connection. When opening a domain with an untrusted certificate in a browser, Kaspersky Endpoint Security displays an HTML page showing the reason why that domain is blocked.

Setting	Description
`EncryptedConnectionsScanErrorAction`	Action on an encrypted connection scan error: `AddToAutoExclusions` (default). When an encrypted connection scan error occurs, the application adds the domain that resulted in the error to the list of exclusions and does not monitor encrypted network traffic when this domain is visited. `Disconnect`. When an encrypted connection scan error occurs, Kaspersky Endpoint Security blocks the network connection.

How to configure monitored ports

While Kaspersky Endpoint Security is running, the Network Threat Protection component monitors data transmitted through some network ports. The list of network ports monitored by the application is configured in accordance with the recommendations of Kaspersky experts.

The Behavior Detection and Exploit Prevention components additionally monitor network ports for application processes that may threaten the security of the computer. The application gets information about such processes with anti-virus databases.

You can configure the ports that you want the application to monitor:

- **Monitor all network ports**. Network port monitoring mode in which the application monitors the data streams passing through any open network ports of the computer.

  Specifying this value may significantly increase an operating system load.

- **Monitor selected network ports only**. In this network port monitoring mode, the protection components monitor the selected ports of the computer and the network activity of the selected applications.

If you want to intercept network connections to the NFS server, you need to make sure that the NFS server is started with the `insecure` option (so that it accepts connections from ports outside the 1–1024 range), otherwise the NFS server may reject such connections.

How to configure monitored ports in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Network Settings**.
5. Under **Monitored ports**, select the application port monitoring mode:
   - **Monitor all network ports**.
   - **Monitor selected network ports only** (default value).

6. If you selected the **Monitor selected network ports only** option, configure the list of ports to monitor:

   a. Click the **Monitored ports** link.

   b. Edit the list of monitored ports.

   > For the Mail Threat Protection component to work, network ports 25, 110, 143, 465, 587, 993, and 995 must be monitored in the network settings. These network ports are added to the list of monitored ports by default. Removing these ports from the list may prevent the component from working correctly.

7. Save your changes.

How to configure monitored ports on the command line

1. To select a port monitoring mode, run the following command:

   ```
   kesl-control --set-net-settings MonitorNetworkPorts=<All|Selected>
   ```

2. If you have opted to monitor only selected ports (`MonitorNetworkPorts=Selected`), specify the list of ports to monitor:

   ```
   kesl-control --set-net-settings NetworkPorts.item_#.PortName=<port name> NetworkPorts.item_#.Port=<port number>
   ```

   To remove a port from the monitoring list, edit the list using a configuration file.

3. To check the current values of network settings, run the following command:

   ```
   kesl-control --get-net-settings
   ```

Symbols

Command options

Setting	Description
`MonitorNetworkPorts`	`Selected` (default value) — Monitor only network ports specified in the `[NetworkPorts.item_#]` section (see below). `All` — Monitor all network ports. Specifying this value may significantly increase an operating system load.
`PortName`	Network port description.
`Port`	Network port numbers to be monitored by the application. Possible values: `1 – 65535`. For the Mail Threat Protection component to work, network ports 25, 110, 143, 465, 587, 993, and 995 must be monitored in the network settings. These network ports are added to the list of monitored ports by default. Removing these ports from the list may prevent the component from working correctly.

Exclusions from traffic interception using the tools of the operating system

In Kaspersky Endpoint Security settings, you can configure exclusions from traffic interception by traffic direction, destination IP address and port. If such exclusions are not sufficient to resolve the conflict of the Kaspersky Endpoint Security application with client applications, you can use the special chain of allow rules, kesl_bypass.

The kesl_bypass chain is a special list of rules that Kaspersky Endpoint Security creates in the mangle table of the operating system firewall (iptables/ip6tables). The rules of the kesl_bypass chain make it possible to exclude traffic from interception by Kaspersky Endpoint Security. The kesl_bypass chain is added to the top of the network packet processing process, which means that kesl_bypass rules are processed before all other iptables rules.

In contrast to exclusions that you can connect in Kaspersky Endpoint Security settings, the kesl_bypass chain allows configuring exclusions not only by traffic direction, destination IP address and port, but also by other parameters of connections.

The rules in the kesl_bypass chain can be changed by means of the operating system.

For example, you can add a rule to the kesl_bypass chain by running the following command:

```
iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT
```

This rule allows excluding inbound and outbound HTTP traffic on port 80 at any IP address from interception by Kaspersky Endpoint Security. This can help avoid potential conflict with web services that you trust.

If traffic exclusion rules are configured in the chain, these rules affect the Web Threat Protection, Network Threat Protection, and Web Control components.

When the application is removed, the kesl_bypass rule chain is removed from iptables and ip6tables only if it was empty.

Interception of file operations

The file operation interception mode affects the File Threat Protection and Device Control components, the Execution prevention for objects action and the Removable Drives Scan task.

If the blocking mode of file operation interception is enabled

- For the duration of the scan, the application can block access to files that are being scanned by the File Threat Protection component. If the scan detects no threats in the file, the application allows access to the file. When infected objects are detected, the application performs the actions specified in the **Actions on threat detection** (`ActionOnThreat`) setting of the File Threat Protection component.

- The application can block access to files on the device while the Device Control component is deciding if access to the device can be granted. The application allows access to files if after the scan, Device Control allows access to the device that contains the files.

- The application may block files on the device while Execution Prevention for objects determines whether these files can be executed. The application allows files to run if, as a result of the scan, Execution Prevention for objects permits these files to run.

- The application may block access to files on the removable drive during the scan. If the scan detects no threats in the file, the application allows access to the file. When infected objects are detected, the application performs the actions specified in the **Actions on threat detection** (`ActionOnThreat`) setting of the File Threat Protection component.

If the blocking mode of file operation interception is disabled

- The File Threat Protection component operates in Inform mode regardless of the selected operating mode and allows access to files, performing the scan asynchronously.

- The Device Control component operates in Inform mode, regardless of the selected operating mode, and always allows access to devices.

- The Execution Prevention for objects action operates in Inform mode, regardless of the selected operating mode, and always allows objects to be executed.

- The application always allows access to files on the removable drive and performs the scan asynchronously.

> This mode of file operation interception has less impact on system performance while scanning, but there is a risk that the threat in the file might not get disinfected or deleted. This may happen if, during the scan, the process associated with this file manages to rename the file before the application can make a decision on the status of this file.

By default, the file operation interception blocking mode is enabled.

How to configure the file operation interception mode in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **General Settings** → **Detection Settings**.

5. Under **File operation interception mode**, clear or select the **Block access to files during scans** check box. This check box is selected by default.

6. Save your changes.

How to configure the file operation interception mode on the command line

You can configure the file operation interception mode in the command line using the `FileBlockDuringScan` setting in the general application settings.

To select the file operation interception mode, run the following command:

```
kesl-control --set-app-settings FileBlockDuringScan=<Yes|No>
```

Symbols

Command options

Setting	Description
`FileBlockDuringScan`	`Yes` (default value) to block access to files while they are being scanned by the File Threat Protection and Device Control components, the Execution prevention action, and the Removable Drives Scan task. `No` to allow access to files during the scan. Requests to any file is allowed, scanning is done asynchronously.

Configuring system event interception

You can choose a system event interception mechanism in the Web Console, on the command line, or in the Administration console.

You can manage the settings for intercepting system events only on devices with an operating system that supports the fanotify technology.

Configuring system event interception is not available for devices with an Elbrus CPU.

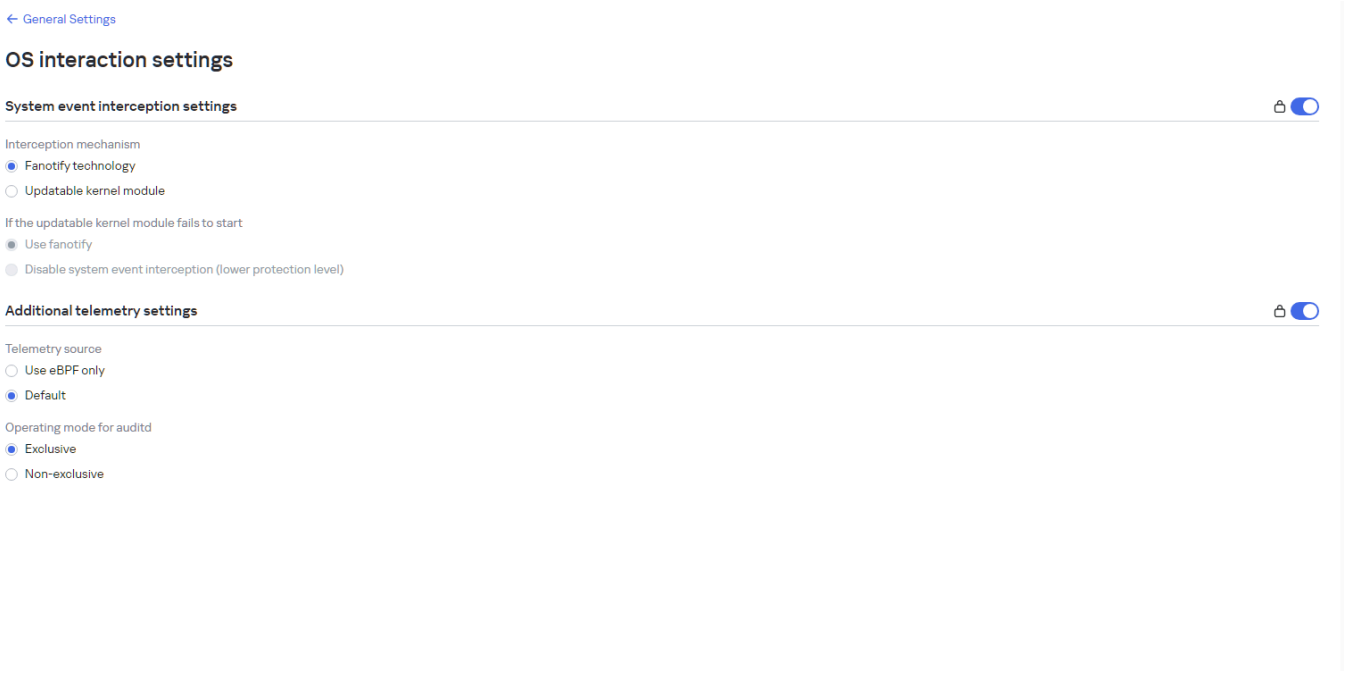
How to configure the system event interception mechanism in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **OS interaction settings**.

5. Under **System event interception settings**, select a system event interception mechanism:

   - **Fanotify technology**.
   - **Updatable kernel module**. If this option is selected, select the action that the application will perform if the updatable kernel module cannot start:
     - **Use fanotify**.
     - **Disable system event interception (lower protection level)**.



OS interaction settings

How to configure the system event interception mechanism on the command line

1. To select a system event interception mechanism, run the following command:

```
kesl-control --set-app-settings InterceptorMode=<UseFanotify|UseUpdatableKernelModule>
```

2. What the application does if the updatable kernel module fails to start, run the following command:

```
kesl-control --set-app-settings InterceptorFallbackStrategy=<FallbackToFanotify|FallbackToLimitedMode>
```

3. To make the application restart when the updatable kernel module fails to start, run the following command:

```
kesl-control --set-app-settings InterceptorApplyStrategy=<RestartServiceAutomatically|RestartServiceManually>
```

4. To check the current application settings, run the following command:

```
kesl-control --get-app-settings [--json]
```

Symbols

Command options

Setting	Description
`InterceptorMode`	`UseFanotify` (default) – use the fanotify technology to intercept system events. `UseUpdatableKernelModule` – use an updatable kernel module to intercept system events.
`InterceptorFallbackStrategy`	`FallbackToFanotify` (default) – switch to fanotify for system event interception. `FallbackToLimitedMode` – do not use system event interception. If the application does not use system event interception, real-time file scanning is not performed, and the protection level of the device is reduced.
`InterceptorApplyStrategy`	`RestartServiceAutomatically` automatically restarts the application to start the updatable kernel module. We recommend using this setting. `RestartServiceManually` (default) starts the updatable kernel module after the application is restarted manually by the user.

The application can use the interception mechanism based on the updatable kernel module if the operating system satisfies the requirements for installing the updatable kernel module.

If you have selected an interception mechanism based on the updatable kernel module, you can configure the application's behavior if an error occurs when the updatable kernel module is started and the module does not start. In this case, the application can fall back to fanotify or disable system event interception.

If the updatable kernel module could not be installed during the installation of the application, you can install it later when support for your operating system becomes available. To do so:

1. Update application databases and modules. The updatable kernel module is installed as part of the regular update procedure.

2. Select the interception mechanism based on the updatable kernel module.

The application can switch to using an updatable kernel module in the following situations:

- In the application settings, you have changed the mechanism for intercepting system events to the updatable kernel module.

- On a device where the updatable kernel module was not started, a database and module update introduced updates that support for the updatable kernel module.

Information about the status of the updatable kernel module

Information about the state and availability of the updatable kernel module is displayed in the form of statuses:

- **Running** means the module is installed and running.

- **Stopped** means the module is installed but not running.

- **Unavailable** means the module is not supported on the device.

- **Malfunction** means an error occurred while starting the module, and the module is not running.

You can view the status of the updatable kernel module on the device in the Web Console and on the command line.

How to view the status of the updatable kernel module in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. In the list of applications installed on the device, click Kaspersky Endpoint Security.

6. View the status of the **Updatable kernel module** functional component.

How to view the status of the updatable kernel module on the command line

To view the status of the updatable kernel module, run the following command:

```
kesl-control --app-info [--json]
```

Where `--json` means output data in JSON format. If you do not specify the `--json` option, settings will be output to the console.

"Safe" mode when using the updatable kernel module

If the application is unstable when using the updatable kernel module, after reaching the specified maximum number of abnormal halts, the application automatically switches to the "safe" mode (`SafeMode=yes` is set in the kesl.ini configuration file). By default, the application enters the "safe" mode after three abnormal halts. The maximum number of abnormal halts is configured in the `PanicThreshold` setting in the kesl.ini configuration file.

If the application is running in "safe" mode, the updatable kernel module does not start, and the application switches to fanotify for intercepting system events. The application sends the `UpdatableKernelModule=Error` tag to Kaspersky Security Center.

To continue using the updatable kernel module after resolving the problems with the application, you need to disable the "safe" mode.

How to disable the safe mode of the application on the command line

1. Open the /var/opt/kaspersky/kesl/common/kesl.ini file for editing.

2. In the `[General]` section, set `SafeMode=no`.

3. Restart Kaspersky Endpoint Security:

   ```
   systemctl restart kesl
   ```

Safe mode is disabled.

Managing additional telemetry settings

You can manage the following advanced settings for the collection of telemetry sent to Detection and Response solutions when integrated with such:

- Telemetry source. You can use the eBPF technology and the auditd service to get telemetry, or the eBPF technology alone.
- The mode of the auditd service. Kaspersky Endpoint Security can use the auditd service in exclusive mode or in multicast mode.

How to configure additional telemetry settings in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **OS interaction settings**.
5. Under **Telemetry settings**, specify the source that Kaspersky Endpoint Security uses to collect telemetry:
   - **Use only eBPF** means only the eBPF technology is used for obtaining telemetry.

     If the **Use only eBPF** option is selected, telemetry for Detection and Response solutions may have limitations.
   - **Default** means the eBPF technology and auditd service are used to get telemetry.
6. Also specify the mode of the auditd service:
   - **Exclusive** means that Kaspersky Endpoint Security uses the auditd service in exclusive mode.
   - **Non-exclusive** means the auditd service is used in non-exclusive mode.

     This setting is applied only if **Telemetry source** is set to **By default**.
7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to configure additional telemetry settings on the command line

On the command line, you can manage additional telemetry settings using the `TelemetrySource` and `UseTelemetryMonopolyMode` settings of the Behavior_Detection predefined task.

1. To enable the telemetry source, run the following command:

```
kesl-control --set-settings 20 TelemetrySource=<Default|OnlyEBPF>
```

2. To select a mode for the auditd service, run the following command:

```
kesl-control --set-settings 20 UseTelemetryMonopolyMode=<True|False>
```

Symbols

Command options

Setting	Description
`TelemetrySource`	`Default` (default) means the eBPF technology and auditd service are used to get telemetry. `OnlyEBPF` means that only the eBPF technology is used to get telemetry.
`UseTelemetryMonopolyMode`	`True` (default) means Kaspersky Endpoint Security uses the auditd service in exclusive mode. `False` means the auditd service is used in non-exclusive mode. The `UseTelemetryMonopolyMode` setting is applied only if `TelemetrySource` is set to `Default`.

Backup

If Kaspersky Endpoint Security detects malicious code in a file while scanning a protected device, the application can block the file, assign to it a status of *Infected*, place a copy in Backup, and attempt to disinfect the file.

Backup keeps copies of files that have been deleted or modified during disinfection. A *backup copy* is created before disinfecting or deleting the file. Backup copies of files are stored in a special format and do not pose a threat.

Sometimes it is not possible to maintain the integrity of files during disinfection. If after disinfection, you partially or completely lose access to important information in a disinfected file, you can try restoring the file from the backup copy.

Restoring infected objects may lead to a device infection.

Backup file copies may contain personal data. Root privileges are required to access Backup objects.

Configuring Backup settings

You can manage Backup settings on a device in the Web Console, in the Administration Console or using the command line. You can configure the following Backup settings:

- **Storage time for objects in Backup.** Objects are kept for 30 days by default. After expiration of the maximum storage term, Kaspersky Endpoint Security deletes the oldest files from Backup.
- **Maximum Backup size.** By default, the following maximum Backup size is configured:
  - 0 MB if a policy is not applied
  - 1024 MB if a policy is applied

  To avoid exceeding the maximum storage size, Kaspersky Endpoint Security automatically deletes the oldest files from storage when the maximum storage size is reached.
- **Path to the directory where Backup and Quarantine objects are stored** (can only be configured on the command line). By default, the /var/opt/kaspersky/kesl/common/objects-backup/ directory is used to store backup copies of files and quarantined files.

How to configure Backup settings in the Web Console

To manage Backup settings in the policy properties:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **General Settings** → **Reports and Storage** section.
5. In the **Backup** section, configure the following settings:
   - **Delete objects after (days)**. If the check box is selected, the maximum file storage term is limited to the defined time interval. This check box is selected by default.

     Valid values are 0 to 10000.
   - **Limit the size of Backup to (MB)**. If the check box is selected, the maximum storage size is limited to the defined value. This check box is selected by default.

     Valid values are 1 to 4000.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

To manage Backup settings in the properties of the managed device:

1. In the main window of the Web Console, select **Asset management** → **Assets (Devices)**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To select a nested group, click the **Show hierarchy** button in the upper part of the window.

   The list displays only the managed devices for the selected administration group.

3. Click the name of a device.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. Select Kaspersky Endpoint Security

6. Go to **Application settings** → **Storage settings**.

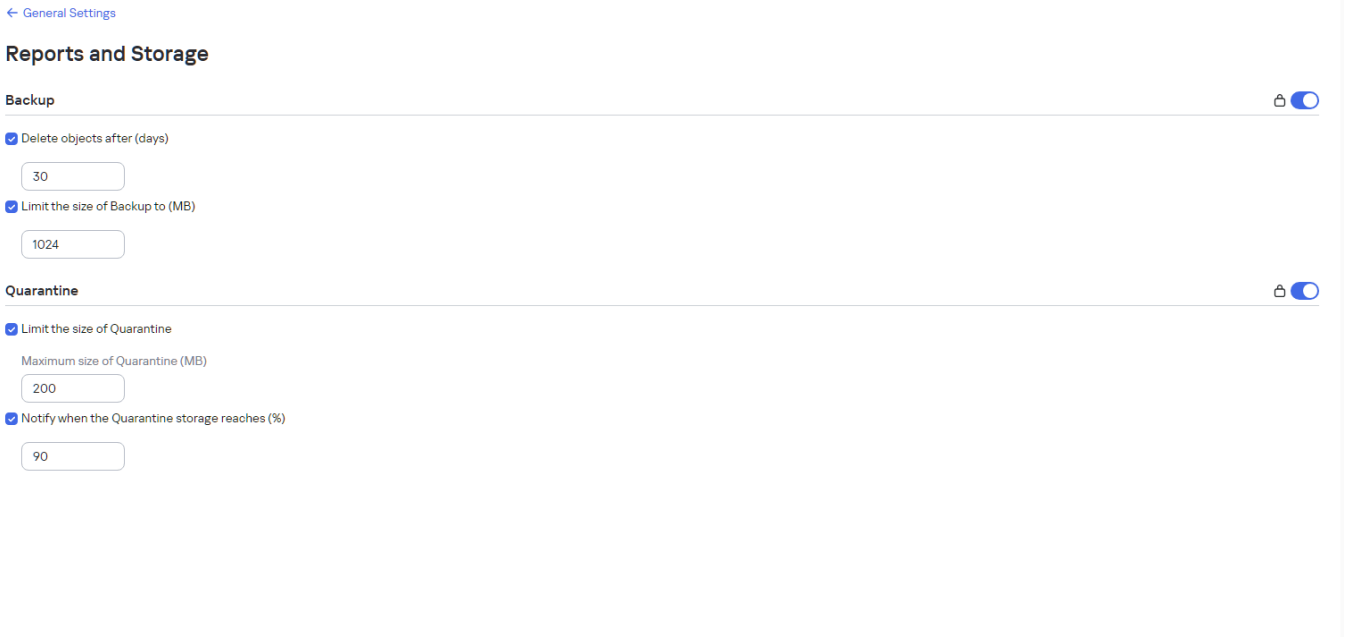
   - **Delete objects after (days)**. If the check box is selected, the maximum file storage term is limited to the defined time interval. This check box is selected by default.

     Valid values are 1 to 10000.

   - **Limit the size of Backup to (MB)**. If the check box is selected, the maximum storage size is limited to the defined value. This check box is selected by default.

     Valid values are 1 to 4000.

7. Save your changes.



Reports and Storage

How to configure Backup on the command line

On the command line, you can configure Backup settings using the `BackupDaysToLive, BackupSizeLimit` and `QuarantineBackupFolder` settings in the general application settings.

1. To configure the retention period for objects in Backup, run the following command:

```
kesl-control --set-app-settings BackupDaysToLive=<days>
```

2. To configure the maximum size of Backup, run the following command:

```
kesl-control --set-app-settings BackupSizeLimit=<Backup size>
```

3. To configure the directory in which the Backup and Quarantine objects are stored, run the following command:

```
kesl-control --set-app-settings QuarantineBackupFolder=<path to folder>
```

4. To check the current application settings, run the following command:

```
kesl-control --get-app-settings
```

Command options

Setting	Description
`BackupDaysToLive`	Time period for storing objects in the Backup storage (in days). After the specified time has elapsed, the application deletes the oldest backup copies of files. To remove the object retention limit, set 0.
`BackupSizeLimit`	Maximum Backup size in MB. When the maximum Backup storage size is reached, the application deletes the oldest backup copies of files. To remove the Backup size limit, set 0.
`QuarantineBackupFolder`	Path to the directory in which the Backup and Quarantine objects are stored. You can specify a directory that is different from the default directory. You can use a directory on any device as the directory for storing Backup and Quarantine objects. It is not recommended to assign directories that are located on remote devices, such as those mounted via the Samba and NFS protocols. If the specified directory does not exist or is unavailable, the application uses the default directory. Default value: `/var/opt/kaspersky/kesl/common/objects-backup/` Root privileges are required for access to the default directory.

Viewing Backup objects

A general list of files placed in Backup by Kaspersky applications on client devices is generated in Kaspersky Security Center and is available in the Web Console and in the Administration Console (**Advanced** → **Repositories** → **Backup**).

Kaspersky Security Center does not copy files from Backup to the Administration Server; all files are stored in the Backups on protected devices.

How to view information about objects in the Backup in the Web Console

1. In the main Web Console window, select **Repositories** → **File backups**.

   This opens a list of files placed in Backup by Kaspersky applications on client devices. Kaspersky Security Center does not copy files from Backup to the Administration Server; all files are stored in the Backups on protected devices.

2. View the properties of files in backup storage on protected devices:

   - **File name**
   - **Status**:
     - *Warning*
     - *Probably infected*

    - *Added by user*
    - *False positive*
    - *Disinfected*
    - *Not infected*
    - *Password-protected*
    - *Deleted*
    - *Must be sent to Kaspersky*
- **Device name**
- **Performed action**:
    - *Deletion*
    - *Disinfection*
    - *Scanning*
    - *Restoring*
- **Object**
- **Placed in repository**
- **Entry added by**
- **Size (bytes)**
- **Folder restored**
- **User**
- **Description**
- **Name of the virtual Administration Server**

How to view information about objects in the Backup on the command line

To view the details of the objects in Backup, run:

```
kesl-control -B --query ["<filter conditions>"] [-n <objects number>] [--json]
```

Where:

- `<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operator> '<value>'` format combined using the logical operator `and` to restrict the results of the query. If you do not specify any filter conditions, the application will display the details of all objects in Backup.

- `<objects number>` specifies how many of the latest objects in storage you want to display. If you do not specify the `-n` option, the application displays information about the last 30 objects. If you want to display information about all objects, specify `0`.

- `--json`: output data in JSON format.

The `ObjectId` line displays the numeric identifier that the application assigned to the object when placing it in Backup. This ID is used to perform actions on the object, such as restoring or removing the object from the Backup storage.

How to view information about objects in the Backup in the graphical interface

1. Open the main window of the application graphical interface.

2. In the lower part of the main application window, click the **Backup** button.

   This opens the **Backup** window.

In this window the following information about the objects in Backup storage is displayed:

- Object name.

- Full path to an object.

- The date when the object was added to Backup.

- The date when the object was deleted from Backup (this field is displayed if Backup retention period is set).

- Object size.

Restoring objects from Backup

The file is restored from Backup to its original location in accordance with to the specified settings. Restoration preserves the MAC label (only on Astra Linux devices) and attributes of the original file (other than the immutable and append-only attributes).

On Astra Linux devices, restoring a file from Backup ends with an error in the following cases:

- The MAC label of the file is higher than the MAC label of the directory to which the file is being restored.

- The MAC label of the file is lower than the MAC label of the directory to which the file is being restored, and the ccnr flag is not set for the directory.

- On Astra Linux devices in the closed software environment mode, you can restore a file only under the same account under which it was placed in Backup. When restoring a file, the application creates a directory with MAC label 3 (cnnr flag).

To manage files in Backup in Kaspersky Security Center, you need to enable the transfer of data about files in Backup to the Administration Server.

Restoring infected objects may lead to a device infection.

How to restore objects from Backup in the Web Console

1. In the main Web Console window, select **Repositories** → **File backups**.

   This opens a list of files placed in Backup by Kaspersky applications on client devices. Kaspersky Security Center does not copy files from Backup to the Administration Server; all files are stored in the Backups on protected devices.

2. Select the check boxes next to the files that you want to restore.

3. Click **Restore**.

Backup objects on client devices are restored.

How to restore objects from Backup on the command line

To restore an object under its original name to its original location, execute the following command:

```
kesl-control -B --restore <object id>
```

Where `<object id>` is the numeric identifier that the application assigned to the object when placing it in Backup.

To restore an object under a new name to the specified directory, execute the following command:

```
kesl-control -B --restore <object id> --file <path to file>
```

Where `--file <path to file>` is the new name of the file and the path to the directory you want to save it to. If the specified directory does not exist, the application creates it.

On Astra Linux devices in the closed software environment mode, you can restore a file only under the same account under which it was placed in Backup.

How to restore objects from Backup in the graphical interface

To restore objects from Backup to their original directories:

1. Open the main window of the application graphical interface.

2. In the lower part of the main application window, click the **Backup** button.

   This opens the **Backup** window.

3. Select the objects that you want to restore.

4. Click **Restore**.

The objects from Backup are restored and become available in the original directory.

Information about restoring and deleting objects is saved to the event log.

Deleting objects from Backup

When the specified retention period expires, or when the maximum Backup size is reached, the application automatically deletes the oldest backup copies regardless of their status.

You can delete the backup copy of a restored or unrestored file manually.

How to delete objects from Backup in the Web Console

1. In the main Web Console window, select **Repositories** → **File backups**.

   This opens a list of files placed in Backup by Kaspersky applications on client devices. Kaspersky Security Center does not copy files from Backup to the Administration Server; all files are stored in the Backups on protected devices.

2. Select the check boxes next to the files that you want to delete.

3. Click the **Delete** button.

Backup objects on client devices are deleted.

How to delete objects from Backup on the command line

To remove selected objects from Backup, run:

```
kesl-control -B --mass-remove --query "<filter conditions>"
```

Where `<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operator> '<value>'` format combined using the logical operator `and` to restrict the results of the query.

Examples:

```
Remove an object with ID=15
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

```
Remove objects that contain "test" in their names or paths
kesl-control -B --mass-remove --query "FileName like '%test%'"
```

To remove all objects from Backup, run:

```
kesl-control -B --mass-remove
```

How to delete objects from Backup in the graphical interface

1. Open the main window of the application graphical interface.
2. In the lower part of the main application window, click the **Backup** button.
   This opens the **Backup** window.
3. Select the objects that you want to delete.
4. Click the **Delete** button.

Backup objects will be deleted. Deleted objects cannot be restored in the future.

Information about restoring and deleting objects is saved to the event log.

Protection against advanced threats and targeted attacks

Kaspersky Detection and Response solutions are security systems for detecting advanced threats and indicators of attack on different levels of an organization's infrastructure. Detection and Response solutions provide information about the detected threats and let you manage your response to detections.

Kaspersky Endpoint Security interoperates with the following Kaspersky Detection and Response solutions:

- Kaspersky Endpoint Detection and Response Expert (on-premises) on the Open Single Management Platform (OSMP). Integration is provided by the Kaspersky Endpoint Security application component, Endpoint Detection and Response Expert (on-premises) (hereinafter also referred to as *EDR Expert (on-premises)*).
- Kaspersky Endpoint Detection and Response Expert (cloud) on the Open Single Management Platform (OSMP). Integration is provided by the Kaspersky Endpoint Security application component, Endpoint Detection and Response Expert (cloud) (hereinafter also referred to as *EDR Expert (cloud)*).
- Kaspersky Endpoint Detection and Response and Kaspersky Network Detection and Response components on the Kaspersky Anti Targeted Attack Platform. Integration is provided by the following components of the Kaspersky Endpoint Security application:
  - Endpoint Detection and Response Expert (on-premises) (hereinafter also referred to as *EDR Expert (on-premises)*).
  - Network Detection and Response (KATA) (hereinafter also *NDR (KATA)*).
- Sandbox on the Open Single Management Platform (OSMP) or on the Kaspersky Anti Targeted Attack Platform. Integration is provided by the following Kaspersky Endpoint Security component: *Sandbox*.
- Kaspersky Unified Monitoring and Analysis Platform.
- Kaspersky Endpoint Detection and Response Optimum. Integration is facilitated by a Kaspersky Endpoint Security component: Endpoint Detection and Response Optimum (*EDR Optimum*).
- Kaspersky Managed Detection and Response. Integration is facilitated by a Kaspersky Endpoint Security component: Managed Detection and Response (*MDR*).

Detection and Response solutions integration features

- If you are using Kaspersky Endpoint Security in the EDR Agent mode, integration is supported only with Kaspersky Endpoint Detection and Response Expert (on-premises) on the Open Single Management Platform (OSMP) and with Kaspersky Endpoint Detection and Response and Kaspersky Network Detection and Response components on the Kaspersky Anti Targeted Attack Platform.

- When Kaspersky Endpoint Security is integrated with Kaspersky Managed Detection and Response and Kaspersky Anti Targeted Attack Platform, the built-in agent may log a large number of events to the systemd-journald log. If you want to disable the logging of audit events to the systemd-journald log, disable the systemd-journald-audit socket and restart the operating system.

  Disable the systemd-journald-audit socket

  ```
  systemctl stop systemd-journald-audit.socket
  systemctl disable systemd-journald-audit.socket
  systemctl mask systemd-journald-audit.socket
  ```

- In the SintezM-Client operating system, the auditd service configuration is protected from modification by default, that is, it is in `enabled 2` mode. For correct operation of the Behavior Detection component when Kaspersky Endpoint Security is integrated with Kaspersky Managed Detection and Response and Kaspersky Anti Targeted Attack Platform solutions, change the auditd mode in the configuration files to `enabled 1` (no configuration blocking) and restart the operating system.

- Detection and Response solutions may not work correctly on virtual machines created from an image with Kaspersky Endpoint Security for Linux installed. When integrating with Detection and Response solutions, a unique ID (Sensor ID) of the computer is used. The application generates this ID as part of the initial installation, and it is retained even after the application is uninstalled. When cloning an image, the virtual machine inherits the Sensor ID, which may cause Detection and Response solutions to identify multiple virtual machines as the same device.

  Recommendations for creating a reference image for correct integration with MDR

  How to prepare a reference image for correct integration with EDR Expert (on-premises)

Response actions

When integrated with Detection and Response solutions, Kaspersky Endpoint Security can perform threat response actions to maintain security functionality. Threat response actions can be generated on the side of the Detection and Response solution and automatically performed on Kaspersky Endpoint Security devices if this functionality is enabled in the settings of the Detection and Response solution. You can also configure and perform threat response actions manually.

> The settings of threat response actions vary depending on the Detection and Response solution with which Kaspersky Endpoint Security is integrated.

Kaspersky Endpoint Security can perform the following threat response actions:

- Isolate the device from the network.

When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response Expert (cloud), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, network isolation is enabled or disabled on the side of the Detection and Response solution. You can manually disable network isolation of a device.

When integrated with Kaspersky Endpoint Detection and Response Optimum, the device can be isolated from the network automatically or manually. You can configure network isolation or manually disable network isolation for a device.

- Quarantine file.

  The action is performed using the *Quarantine file* task.

  When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, the tasks are created and run on the side of the Detection and Response solution.

  When integrated with Kaspersky Endpoint Detection and Response Optimum, a file can be quarantined automatically as a result of detection of indicators of compromise.

  When integrated with Kaspersky Endpoint Detection and Response Optimum or with Kaspersky Managed Detection and Response, you can also manually quarantine files.

- Restore files from Quarantine.

  When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response Expert (cloud), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, the threat response action is generated on the side of the Detection and Response solution. You can also perform the action manually using Kaspersky Security Center or the command line.

  When integrated with Kaspersky Endpoint Detection and Response Optimum, you can perform the action manually using Kaspersky Security Center or the command line.

- Delete a file from Quarantine.

  When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response Expert (cloud), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, the threat response action is generated on the side of the Detection and Response solution. You can also perform the action manually using Kaspersky Security Center or the command line.

  When integrated with Kaspersky Endpoint Detection and Response Optimum, you can perform the action manually using Kaspersky Security Center or the command line.

- Get a file from Quarantine.

  When integrated with Kaspersky Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response Expert (cloud), or with Kaspersky Endpoint Detection and Response (KATA), the threat response action is generated on the side of the Detection and Response solution.

  When integrated with Kaspersky Endpoint Detection and Response Optimum, you can perform the action manually using Kaspersky Security Center.

- Receive file from device.

  This action is performed using the *Get file* task. For example, you can configure the application to get an event log file generated by a third-party application.

  When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, the tasks are created and run on the side of the Detection and Response solution.

  When integrating with the Kaspersky Endpoint Detection and Response Optimum solution, you can create Get file tasks in the Web Console.

- Delete file from device.

  This action is performed using the *Delete file* task.

  When integrated with Kaspersky Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response Expert (cloud), or with Kaspersky Endpoint Detection and Response (KATA), the task is created and run on the side of the Detection and Response solution.

  When integrating with the Kaspersky Endpoint Detection and Response Optimum solution, you can create Delete file tasks in the Web Console.

- Remotely run a process on a device.

  This action is performed using the *Run application* task. For example, you can remotely run a utility that creates a device configuration file, and then retrieve the created file using the *Get file* task.

  When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, the tasks are created and run on the side of the Detection and Response solution.

  When integrating with the Kaspersky Endpoint Detection and Response Optimum solution, you can create and run Run process tasks in the Web Console.

- Remotely terminate a process on a device.

  The action is performed using the *Kill process* task. For example, you can remotely terminate an Internet speed test utility that was launched using the "Run process" task.

  When integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, the tasks are created and run on the side of the Detection and Response solution.

  When integrating with the Kaspersky Endpoint Detection and Response Optimum solution, you can create and run Kill process tasks in the Web Console.

- Detecting indicators of compromise (IOC) on devices.

  An *Indicator of Compromise (IOC)* is a set of data about an object or activity that indicates unauthorized access to a device (compromised data). For example, an indicator of compromise could be a high number of failed login attempts.

- Starting a *YARA scan*.

  During a *YARA scan*, Kaspersky Endpoint Security uses YARA files to search for signatures of malicious activity on a device. *YARA files* are files with the .YARA or .YAR extension that contain YARA rules. *YARA rules* describe signatures of targeted attacks and intrusions into corporate IT infrastructure. Kaspersky Endpoint Security uses these rules to scan objects. If the conditions of a rule is satisfied, the analyzer concludes that an infection is ongoing, and records the detail in the log. The scan is performed recursively on local drives. Scanning of network, removable, and cloud resources is not supported.

  The command for a YARA scan on a Kaspersky Endpoint Security device is created and run on the side of the Kaspersky Endpoint Detection and Response Expert (on-premises) and Kaspersky Endpoint Detection and Response Expert (cloud) solutions.

- Execution prevention

- Getting forensics.

  When integrated with Kaspersky Endpoint Detection and Response Expert (on-premises) and Kaspersky Endpoint Detection and Response Expert (cloud), you can collect digital data that may be useful when investigating incidents related to cybercrimes and data leaks.

This action can be performed using the following tasks:

- The *Get forensics* task, which collects the following types of information:
  - List of files
  - List of processes
  - List of autorun points
- *Get memory dump* tasks
- *Get process memory dump* tasks
- *Get disk image* tasks

Tasks are created and run on the side of the Kaspersky Endpoint Detection and Response Expert (on-premises) and Kaspersky Endpoint Detection and Response Expert (cloud) solutions.

Searching for indicators of compromise

An *Indicator of Compromise (IOC)* is a set of data about an object or activity that indicates unauthorized access to the computer (compromise of data). For example, an indicator of compromise could be a high number of failed login attempts. The *IOC Scan* task allows finding Indicators of Compromise on the computer and taking threat response measures.

The IOC Scan functionality is available in the Kaspersky Endpoint Security application if one of the following conditions is satisfied:

- Integration of Kaspersky Endpoint Security with the Kaspersky Endpoint Detection and Response Optimum solution is enabled and the EDR Optimum component is activated.

  In this case, IOC search is performed using the *IOC Scan* task.

- Integration of the Kaspersky Endpoint Security application with the Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA) component is enabled, and the EDR Expert (on-premises) component is activated.

  In this case, the IOC scan is performed on the side of the corresponding solution.

The *IOC Scan* task checks for IOC terms (properties of IOC objects, for example, a file hash) only in the operating system's main namespace. The *IOC Scan* task does not calculate hashes of files larger than 200 MB.

To search for indicators of compromise, Kaspersky Endpoint Security uses IOC files prepared by the user. If you want to add an indicator of compromise manually, please see IOC file requirements. If the IOC file does not meet the requirements, the application will not be able to use it.

IDs of all IOC files used in an IOC Scan task must be unique. If you load multiple IOC files with the same ID, the application only uses one of those IOC files. The other IOC files will be automatically excluded.

Creating an IOC Scan task

You can create *IOC Scan* tasks manually:

- In alert details (only for EDR Optimum).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. For details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help and the Kaspersky Endpoint Detection and Response Expert Help.

- Using the Task Wizard.

- Locally on the command line.

How to create an IOC Scan task in the Web Console

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux 12.5**.

   b. In the **Task type** drop-down list, select **IOC Scan**.

   c. In the **Task name** field, enter a name for the new task.

   d. Under **Devices to which the task will be assigned**, select how you want to define a scope for the task.

4. Select devices according to your preferred task scope definition method. Proceed to the next step.

5. Finish the wizard.

   A new task will be displayed in the list of tasks.

6. Click the new task.

   The task properties window opens.

7. Select the **Application settings** tab.

8. Go to the **Threat Scan** section.

9. Upload the IOC files to search for indicators of compromise.

   After you upload the IOC files, the application displays summary information about the file, including the list of indicators that did not pass the check. After uploading IOC files, you can manually edit the files in the built-in editor directly in task properties. Kaspersky Endpoint Security supports editing IOC files that are compliant with the OpenIOC 1.1 standard. It is not possible to modify the content of IOC files compliant with OpenIOC version 1.0.

Kaspersky Endpoint Security adds IOC files to the IOC collection. If necessary, you can temporarily exclude IOC files from the task scope.

> We do not recommend adding or deleting IOC files after starting this task. This may result in incorrect display of IOC scan results for previous runs of the task. We recommend adding a new task to run an IOC scan based on new IOC files.

10. Go to the **Scan settings** section.

11. If necessary, configure Retrospective IOC Scan.

    Retrospective IOC Scan is a mode of the *IOC Scan* task in which Kaspersky Endpoint Security scans for indicators of compromise using data for a certain time period. This mode is intended for searching indicators of compromise by the telemetry of the protected computer such as network activity, processes, files, and other telemetry. Kaspersky Endpoint Security analyzes data in operating system logs and browser logs on the computer. The Retrospective IOC Scan analyzes logs of the following browsers: Google Chrome, Mozilla Firefox, Microsoft Edge (version 79 or later).

    a. Under **Retrospective IOC Scan**, go to search settings.

    b. Enable the **Retrospective IOC Scan** toggle switch.

    c. Set the time interval for retrospective IOC scans.

12. Select data types (IOC documents) that must be analyzed as part of the task.

    > Kaspersky Endpoint Security automatically selects data types (IOC documents) for the *IOC Scan* task in accordance with the content of loaded IOC files. It is not recommended to deselect data types.

    Additionally, you can configure the search scopes for the **Files - FileItem** data type. Set an IOC scan scope on the computer using preset scopes.

13. Go to the **Response settings** section.

14. Select the task operating mode: **Alert only** or **Alert and response**.

15. Select a response action for when an IOC is detected:

    - **Run Critical Areas Scan**. If this option is selected, Kaspersky Endpoint Security runs the *Critical Areas Scan* task. By default, Kaspersky Endpoint Security scans the kernel memory, running processes, and boot sectors.

      Critical areas scanned by Kaspersky Endpoint Security

      - /lib/systemd
      - /lib/udev
      - /lib/dbus-1.0
      - /usr/local/lib/systemd/user
      - /usr/share/dbus-1

- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron
- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

- **Move copy to Quarantine, delete object**. If this option is selected, Kaspersky Endpoint Security deletes the malicious object found on the computer. Before deleting an object, Kaspersky Endpoint Security creates a backup copy of it in case you need to restore the object later. Kaspersky Endpoint Security moves the backup copy to Quarantine.

  If this check box is cleared, you can quarantine the file manually after running the task manually. If the *IOC Scan* task detects a file that can compromise data, you can quarantine this file directly from IOC Scan results (**Application settings** → **IOC Scan results**). As a result, Kaspersky Endpoint Security starts the task creation wizard with preset data of the detected file. You only need to manage additional task settings, for example, set up the task schedule.

- **Isolate device from the network**. If this option is selected, Kaspersky Endpoint Security isolates the computer from the network to prevent the threat from spreading. You can configure the duration of the isolation in Endpoint Detection and Response component settings.

  If this check box is cleared, you can isolate the computer from the network after running the task manually. If the *IOC Scan* task detects a file that can compromise data, you can quarantine this file directly from IOC Scan results (**Application settings** → **IOC Scan results**). As a result, Kaspersky Endpoint Security starts the task creation wizard with preset data of the detected file. You only need to manage additional task settings, for example, set up the task schedule.

16. In the task properties window, select the **Schedule** tab.

17. Configure the task schedule.

    Wake-on-LAN is not available for this task. Make sure the computer is turned on to run the task.

18. Save your changes.

19. Select the check box next to the task.

20. Click **Start**.

You can view the result of the *IOC Scan* task in the task properties in the Web Console under **IOC Scan results**. IOC Scan results are stored for 30 days. After this time expires, Kaspersky Endpoint Security automatically deletes old entries.

How to create an IOC Scan task on the command line

Execute the command:

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Symbols

Settings of the Malware Scan task

Setting	Description
`--path`	Path to IOC file or directory with IOC files with the .IOC or .XML extension, which should be used to perform the scan. *IOC files* are files containing the sets of indicators that the application tries to match to count a detection. IOC files must conform to the OpenIOC standard. You can specify multiple paths by separating them with a space. You can also specify both types of paths (path to a file and path to a directory).
`--process`	Analyze process data when performing the IOC scan (ProcessItem term). If the value of the argument is `off`, Kaspersky Endpoint Security does not analyze processes running on the computer when performing the scan. If the IOC file contains IOC terms of the ProcessItem IOC document, they are ignored (detected as no match). If the argument is not specified, Kaspersky Endpoint Security analyzes process data only if the ProcessItem IOC document is described in the IOC file that is provided for the scan.
`--hint`	Analyze files data when performing the IOC scan (ProcessItem and FileItem terms). You can select a file in one of the following ways: • `<full path to the executable file of the process>` – ProcessItem term; • `<full path to the file>` – FileItem term.
`--arpentry`	Analyze the data about records in the ARP table when performing the IOC scan (ArpEntryItem term). If the value of the argument is `off`, Kaspersky Endpoint Security does not scan the ARP table. If the IOC file contains ArpEntryItem IOC document terms, they are ignored (detected as no match). If the argument is not specified, Kaspersky Endpoint Security analyzes the ARP table only if the ArpEntryItem IOC document is described in the IOC file that is provided for the scan.
`--ports`	Analyze data about ports open for listening when performing the IOC scan (PortItem term). If the value of the argument is `off`, Kaspersky Endpoint Security does not scan the table of active connections on the device. If the IOC file contains PortItem IOC document terms, they are ignored (detected as no match). If the argument is not specified, Kaspersky Endpoint Security analyzes the table of active connections only if the PortItem IOC document is described in the IOC file that is provided for the scan.
`--system`	Analyze environment data when performing the IOC scan (SystemInfoItem term). If the value of the argument is `off`, Kaspersky Endpoint Security does not analyze environment data. If the IOC file contains SystemInfoItem IOC document terms, they are ignored (detected as no match). If the argument is not specified, Kaspersky Endpoint Security analyzes environment data only if the SystemInfoItem IOC document is described in the IOC file that is provided for the scan.
`--files`	Analyze file data when performing the IOC scan (FileItem term). If the value of the argument is `off`, Kaspersky Endpoint Security does not analyze file data. If the IOC file contains FileItem IOC document terms, they are ignored (detected as no match). If the argument is not specified, Kaspersky Endpoint Security analyzes file data only if the FileItem IOC document is described in the IOC file that is provided for the scan.
`--drives`	Set IOC scan scope when analyzing data for the FileItem IOC document. You can set the following values for the scan scope: • `<all>` for all available file scopes. • `<system>` for files in folders where the operating system is installed. • `<critical>` for temporary files in user and system folders. • `<custom>` for files in user-defined scopes (`/scope=<list of folders to scan>`). If the argument is not specified, the scan is performed for critical areas.
`--excludes`	Set exclusion scope when analyzing data for the FileItem IOC document. You can specify multiple paths separated by spaces.
`--scope`	User-defined IOC scan scope when analyzing data for the FileItem IOC document (`/drives=custom`). You can specify multiple paths separated by spaces.
`--action`	Action performed when indicators of compromise are detected: • `Skip`. If this option is selected, Kaspersky Endpoint Security only detects files that can cause data compromise. • `QuarantineFile`. If this option is selected, Kaspersky Endpoint Security deletes the malicious object found on the computer. Before deleting an object, Kaspersky Endpoint Security creates a backup copy of it in case you need to restore the object later. Kaspersky Endpoint Security moves the backup copy to Quarantine. • `IsolateHost`. If this option is selected, Kaspersky Endpoint Security isolates the computer from the network to prevent the threat from spreading. • `ScanCriticalAreas`. If this option is selected, Kaspersky Endpoint Security runs the *Critical Areas Scan* task. By default, Kaspersky Endpoint Security scans the kernel memory, running processes, and boot sectors.

Network isolation

When integrated with Detection and Response solutions, a device can be isolated from the network as part of a threat response action.

Special considerations involved with network isolation

After enabling network isolation, the application severs all active network connections on the device and blocks all new TCP/IP network connections, except for the connections listed below:

- Connections specified in exclusions from network isolation
- Connections initiated by Kaspersky Endpoint Security services
- Connections initiated by the Kaspersky Security Center Network Agent
- Connections to the SVM and the Integration Server if the application is being used in Light Agent mode.
- KSN connections (when integrated with Kaspersky Managed Detection and Response)

Network isolation can be applied when one of the following conditions is satisfied:

- Integration of Kaspersky Endpoint Security with the Kaspersky Endpoint Detection and Response Optimum solution is enabled and the EDR Optimum component is activated.
- Integration of the Kaspersky Endpoint Security application with the Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA) component is enabled, and the EDR Expert (on-premises) component is activated.
- Integration of Kaspersky Endpoint Security with the Kaspersky Managed Detection and Response solution is enabled and the MDR component is activated.

When integrated with Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Detection and Response (KATA), and Kaspersky Managed Detection and Response, network isolation of a device is enabled or disabled, and network isolation exclusions are configured on the side of the Detection and Response solution. For details, see the Kaspersky Endpoint Detection and Response Expert (on-premises) Help, the Kaspersky Anti Targeted Attack Platform Help, or the Kaspersky Managed Detection and Response Help. If necessary, you can manually disable network isolation of a device:

- In the device properties in the Web Console (only when integrated with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA))
- On the command line

Manually disabling network isolation is possible regardless of whether integration with Detection and Response solutions is enabled, and regardless of whether a policy is applied to the device.

When integrated with Kaspersky Endpoint Detection and Response Optimum, network isolation can be applied in one of the following modes:

- Automatic network isolation mode. A device can be isolated from the network automatically as a result of detection of indicators of compromise. When creating and configuring *IOC Scan* task settings in the **Actions on IOC detection** section, if you select the **Apply response actions when an IOC is detected** and **Isolate device from the network** check boxes, then network isolation is enabled automatically when the application detects indicators of compromise.

  You can manage the following automatic network isolation settings:

  - Change the period of time after which network isolation is automatically disabled.
  - Configure network isolation exclusions for automatically isolated devices.

  > If a device that is being isolated automatically is subject to a policy, the settings specified in the policy are applied. If a policy is not applied, the settings specified in the device properties are applied.

- Manual network isolation mode. You can isolate a device from the network while the detected threat is being investigated. You can manually enable network isolation for a device in the alert details window and in the device properties in the Web Console.

  You can manage the following manual network isolation settings:

  - Change the period of time after which network isolation is automatically disabled.
  - Configure network isolation exclusions for manually isolated devices.

When integrated with Kaspersky Endpoint Detection and Response Optimum, you can manually disable network isolation of a device in the device properties in the Web Console and on the command line.

You can check the network isolation status of a device on the command line.

An isolated device is automatically assigned the **ISOLATED FROM NETWORK** tag. This tag is automatically removed when network isolation is disabled.

For general information on getting a list of isolated devices by tag, see the Kaspersky Endpoint Detection and Response Optimum Help.

Network isolation limitations

> When you use network isolation, we strongly recommended that you familiarize yourself with the relevant limitations.

For network isolation to work, Kaspersky Endpoint Security must be running. If Kaspersky Endpoint Security malfunctions (and the application is not running), traffic may not be blocked when network isolation is enabled by Kaspersky Managed Detection and Response.

DHCP and DNS are not automatically added to network isolation exclusions, so if the network address of a resource changes during network isolation, Kaspersky Endpoint Security cannot gain access to it. The same applies to the nodes of the fault-tolerant KATA server. We recommend to not change their addresses so that Kaspersky Endpoint Security does not lose contact with them.

The proxy server is not added automatically to the network isolation exclusions, so you need to add it to the exclusions manually so that Kaspersky Endpoint Security does not lose contact with the server providing the integration.

Excluding a process from network isolation by name is supported on devices with kernel version 4.18 or later with eBPF and BTF support and with tracepoints and kprobes functions enabled for kernel tracing.

If Kaspersky Endpoint Security is being used in standard mode or in EDR Agent mode, when using network isolation, we recommend the following:

- Use a KSN proxy server to interact with Kaspersky Security Network.
- Use Kaspersky Security Center as a proxy server for application activation.

  If it is impossible to use Kaspersky Security Center as a proxy server, you must configure the proxy server that you want to use and add it to exclusions.
- Specify Kaspersky Security Center as the database update source.

These recommendations do not apply if Kaspersky Endpoint Security is used in Light Agent mode.

Manually enabling or disabling the network isolation of the device in the Web Console

You can enable network isolation for a device using Web Console only when integrated with Kaspersky Endpoint Detection and Response Optimum.

Enabling and disabling network isolation of a device manually when integrating with Kaspersky Endpoint Detection and Response Optimum

To manually enable or disable network isolation for a device:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.
2. If necessary, select an administration group, find your device, and click on its name.
3. This opens a managed device properties window; in that window, go to the **Applications** tab.
4. In the list of applications installed on the device, click Kaspersky Endpoint Security.
5. In the application properties window that opens, on the **Application settings** tab, select **Built-in agents** → **Endpoint Detection and Response**.

6. This opens a window; in that window, under **Network isolation**, do one of the following:

   - Click the **Isolate device from the network** button, to enable network isolation of a device. The button is available only if the **Endpoint Detection and Response** toggle switch is enabled.

     When you click this button, the device will be isolated for the period you specified in the properties of the *Enabling network isolation (NetworkIsolationStart)* task.

   - Click the **Unblock an isolated device** button to disable network isolation of the device. The button is available regardless of whether the **Endpoint Detection and Response** toggle switch is enabled or disabled.

7. Click **OK**.

If you enabled network isolation of the device, Kaspersky Endpoint Security assigns the **ISOLATED FROM NETWORK** tag to the device. If you disabled network isolation of a device, Kaspersky Endpoint Security removes this tag from the device.

Manually disabling network isolation of a device when integrating with Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA)

To manually disable network isolation for a device:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To do so, click the link in the **Current path** field above the list of managed devices and select an administration group in the window that opens.

   The list displays only the managed devices for the selected administration group.

3. Find your device in the list and click its name.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. In the list of applications installed on the device, click Kaspersky Endpoint Security.

6. In the application properties window that opens, on the **Application settings** tab, select the **Detection and Response** section.

7. Under **Network isolation (EDR Expert (on-premises))**, click the **Unblock an isolated device** button to disable network isolation of the device.

After disabling network isolation of a device, Kaspersky Endpoint Security removes the **ISOLATED FROM NETWORK** tag from the device.

Configuring the duration of automatic network isolation

You can configure the duration of automatic network isolation only if integrated with Kaspersky Endpoint Detection and Response Optimum:

Network isolation of devices isolated by the *IOC Scan* task is automatically disabled after a certain length of time. You can configure this timeout in the Web Console in the device properties and in policy properties. The network isolation settings in the policy properties in the Web Console are described in Appendix 5. The network isolation settings in the managed device properties are described in the table below.

If a policy is applied to the device, the settings specified in the policy are applied; the automatic network isolation timeout cannot be configured in the device properties. If a policy is not applied to the device, the settings specified in the device properties are applied.

By default, the application disables network isolation 5 hours after it is enabled. With network isolation disabled, the device can operate on the network without restrictions.

Configuring the automatic disabling of network isolation in the device properties

To configure the automatic disabling of device network isolation:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To do so, click the link in the **Current path** field above the list of managed devices and select an administration group in the window that opens.

   The list displays only the managed devices for the selected administration group.

3. Find your device in the list and click on its name.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. In the list of applications installed on the device, click Kaspersky Endpoint Security.

6. In the application properties window that opens, on the **Application settings** tab, select **Detection and Response** and click the **Endpoint Detection and Response Optimum** link.

7. Under **Network isolation**, click **Configure device unblocking**.

8. This opens the **Configure device unblocking** window; in that window, select the **Unblock an automatically isolated device after** check box and in the input field under it, specify the period in hours after which the device must be automatically unblocked.

9. Save your changes.

Manually configuring network isolation

To manually isolate a device from the network, you need integration with Kaspersky Endpoint Detection and Response Optimum.

If you manually enable network isolation for a device, you can pre-configure network isolation using the *Enabling network isolation* (*NetworkIsolationStart*) local task. You can configure network isolation exclusions and the duration of network isolation for a device.

Enabling network isolation is a predefined task and runs only automatically in the following cases:

- If you click the **Isolate device from the network** button in the device properties.
- If you enable network isolation of the device in the alert details window.

You cannot create a new instance of the *Enabling network isolation* task by clicking the **Add** button or run the task by clicking the **Start** button. This task is only available in the device properties, where you can change its settings before enabling network isolation for the device.

> The *Enabling network isolation* task settings apply regardless of whether a policy is applied to the device.

To configure the network isolation parameters for a device:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. Select the administration group containing the necessary device. To do so, click the link in the **Current path** field above the list of managed devices and select an administration group in the window that opens.

   The list displays only the managed devices for the selected administration group.

3. Find your device in the list and click on its name.

4. This opens a managed device properties window; in that window, go to the **Tasks** tab.

5. In the task list, click the *Enabling network isolation* task.

   The task properties window opens.

6. Go to the **Application settings** tab.

7. Click the **Configure exclusions** link to open the **Exclusions** window.

8. In the window that opens, use the buttons above the table to perform the necessary action:

   - If you want to add information about an excluded network connection, do so in one of the following ways:
     - Click the **Add** button and enter information about the network connection.
     - Click the **Add from profile** button and select a network profile from the dictionary.
   - If you want to delete information about an excluded network connection, select the check box next to the network connection to be removed and click the **Remove** button.

9. Click **OK**.

10. Enter the desired duration of network isolation of the device, in hours, in the **Isolate the device for** field.

    The default duration of network isolation is 5 hours.

    The minimum duration of network isolation is 1 hour.

11. Click the **Save** button to save the changes made.

Configuring exclusions from network isolation in the Web Console

When Kaspersky Endpoint Security is integrated with Endpoint Detection and Response Expert (on-premises), with Kaspersky Endpoint Detection and Response (KATA), or with Kaspersky Managed Detection and Response, exclusions from network isolation are configured on the side of the Detection and Response solution. For details, see the Kaspersky Endpoint Detection and Response Expert (on-premises) Help, the Kaspersky Anti Targeted Attack Platform Help, or the Kaspersky Managed Detection and Response Help.

When Kaspersky Endpoint Security is integrated with Kaspersky Endpoint Detection and Response Optimum, you can configure exclusions from network isolation in the following ways:

- In the policy properties in the Web Console. Exclusions configured in the policy are applied when network isolation is automatically enabled for a device that the policy is applied to.
- In the device properties in the Web Console. Exclusions configured in device properties are applied when network isolation is automatically enabled for a device that no policy is applied to.
- In the settings of the *Enabling network isolation* (*NetworkIsolationStart*) local task. Exclusions configured in the properties of this task are applied when you manually enable network isolation for a device. The *Enabling network isolation* task settings apply regardless of whether a policy is applied to the device.

For configuring exclusions from network isolation, the application provides a list of *standard network profiles*. Network profiles consist of rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles. You can manage the settings of standard network profiles and configure exclusions manually.

> Adding or removing network isolation exclusions in the device properties is not available if a policy is applied to the device.

How to add a Network isolation exclusion in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. In the **Network Isolation** block, click the **Exclusions** link.

   This opens a window with a list of exclusions from network isolation.

6. You can exclude a network connection in the following ways:

   - Click **Add** and enter the information about the network connection.

     You can add an application for which the component will not block network connections. This setting is applicable to devices with kernel version 4.18 or later with eBPF and BTF support and with tracepoints and kprobes functions enabled for kernel tracing.

   - Click the **Add from profile** button and select a network profile from the dictionary.

7. Save your changes.

How to remove a Network isolation exclusion in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. In the **Network Isolation** block, click the **Exclusions** link.

   This opens a window with a list of exclusions from network isolation.
6. Select the check box next to the network connection and click **Delete**.
7. Save your changes.

Quarantine file

When reacting to threats, Kaspersky Endpoint Detection and Response can create *Move file to Quarantine* tasks. This is necessary to minimize the consequences of the threat. *Quarantine* is a special local storage on the computer. The user can quarantine files that the user considers dangerous for the computer. Quarantined files are stored in an encrypted form and do not threaten the security of the device.

You can create *Move file to Quarantine* tasks in the following ways:

- In alert details (only for EDR Optimum).

  Alert Details is a tool for viewing the entirety of collected information about a detected threat. Alert details include, for example, the history of files appearing on the computer. You can select the file to be deleted directly from the alert details. As a result, Kaspersky Endpoint Security starts the task creation wizard with preset data of the detected file. You only need to manage additional task settings, for example, set up the task schedule.

- Using the Task Wizard.

  The New task wizard allows manually entering the path to the file or directory and the hash of the file to be deleted. You can also manage additional task settings, such as setting up the task schedule.

- In the *IOC Scan* task settings.

  If the *IOC Scan* task detects a file that can compromise data, you can quarantine this file directly from IOC Scan results (**Application settings** → **IOC Scan results**). As a result, Kaspersky Endpoint Security starts the task creation wizard with preset data of the detected file. You only need to manage additional task settings, for example, set up the task schedule.

The file size must not exceed 100 MB.

How to create a Move file to Quarantine task

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux**.

   b. In the **Task type** drop-down list, select **Move file to Quarantine**.

   c. In the **Task name** field, enter a brief description.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option. Click **Next**.

5. Finish the wizard by clicking the **Finish** button.

   A new task will be displayed in the list of tasks.

6. Click the new task.

7. The task properties window opens.

8. Select the **Application settings** tab.

9. In the list of files, click **Add**.

   The file adding wizard starts.

10. To add a file, you need to enter the file path or the directory path and the file hash.

11. In the task properties window, select the **Schedule** tab.

12. Configure the task schedule.

13. Save your changes.

14. Select the check box next to the task.

15. Click **Start**.

    As a result, Kaspersky Endpoint Security moves the file to Quarantine.

If the file is locked by a different process, the task is displayed as *Completed*, but the file itself is quarantined only after the computer is restarted. After restarting the computer, confirm that the file is deleted.

The *Move file to Quarantine* task can finish with the *Access denied* error if you are trying to quarantine an executable file that is currently running. Create a terminate process task for the file and try again.

The *Move file to Quarantine* task can finish with the *Not enough space in Quarantine storage* error if you are trying to quarantine a file that is too large. Clear the Quarantine or increase the size of the Quarantine. Then try again.

Receiving a file from a device

You can get files from user computers. For example, you can configure the application to get an event log file generated by a third-party application. As a result of the execution of the task, a file copy is saved in Quarantine. *Quarantine* is a special local storage on the computer. You can download this file from Quarantine to your computer using Web Console (**Operations** → **Repositories** → **Quarantine**). The original file on the user device remains in its original directory.

In Kaspersky Security Center, in the list of quarantined files, all files received through the *Get file* task will have the *Infected* status regardless of the file scan results.

The file size must not exceed 100 MB.

How to create a Get file task

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux**.

   b. In the **Task type** drop-down list, select **Get file**.

   c. In the **Task name** field, enter a brief description.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option. Click **Next**.

5. Finish the wizard by clicking the **Finish** button.

   A new task will be displayed in the list of tasks.

6. Click the new task.
7. The task properties window opens.
8. Select the **Application settings** tab.
9. In the list of files, click **Add**.

   The file adding wizard starts.
10. To add a file, you need to enter the file path or the directory path and the file hash.
11. In the task properties window, select the **Schedule** tab.
12. Configure the task schedule.
13. Save your changes.
14. Select the check box next to the task.
15. Click **Start**.

    As a result, Kaspersky Endpoint Security creates a copy of the file and moves that copy to Quarantine. You can download the file from Quarantine in Web Console.

The *Get file* task finishes with an error if:

- The specified file is not found.
- Incorrect file information (file name or checksum) is specified.
- Insufficient rights to manage the specified file.
- The specified file is blocked.
- Insufficient space in Quarantine.
- The specified file is too big (more than 100 MB).

Delete file from device

You can remotely delete files using the *Delete file* task. For example, you can remotely delete a file when responding to threats.

How to create a Delete file task

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.
2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux**.

   b. In the **Task type** drop-down list, select **Delete file**.

   c. In the **Task name** field, enter a brief description.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option. Click **Next**.

5. Finish the wizard by clicking the **Finish** button.
   A new task will be displayed in the list of tasks.

6. Click the new task.

7. The task properties window opens.

8. Select the **Application settings** tab.

9. To add a file, you need to enter the directory path and the file hash.

10. In the task properties window, select the **Schedule** tab.

11. Configure the task schedule.

12. Save your changes.

13. Select the check box next to the task.

14. Click **Start**.

    As a result, Kaspersky Endpoint Security deletes the file from the computer. If the file is locked by a different process, the task is displayed as *Done*, but the file itself is deleted only after the computer is restarted. After restarting the computer, confirm that the file is deleted.

Start process

You can remotely run files using the *Process start* task. For example, you can remotely run an utility that creates the computer configuration file. Next you can use the *Get file* task to receive the created file in Kaspersky Security Center Web Console.

> If SELinux in your operating system is in `Enforcing` mode, to start the *Process start* task, you need to perform additional configuration of SELinux.

How to configure SELinux to run the "Start process" task

If you plan to use SELinux in the `Enforcing` mode on your operating system, then to perform response actions when integrating with Detection and Response solutions, you need to additionally manage SELinux settings.

> This SELinux configuration requires root privileges.

To configure SELinux for response actions:

1. Switch SELinux to permissive mode:

   - If SELinux is enabled, run the following command:

     ```
     Switch SELinux to permissive mode
     setenforce Permissive
     ```

   - If SELinux is disabled, set `SELINUX=permissive` in the /etc/selinux/config configuration file and restart the operating system.

2. Make sure the semanage utility is installed on the system. If the utility is not installed, install the policycoreutils-python or policycoreutils-python-utils package, depending on the package manager.

3. Run all tasks to perform the response actions that you want to use as part of integration with Detection and Response solutions.

4. Make sure there are no errors in the audit.log file.

   ```
   View the audit.log file
   grep kesl /var/log/audit/audit.log
   ```

5. If any errors are present in the audit.log file, create and load a new rules module based on blocking records to fix the errors, then run the response actions tasks again.

   ```
   Create and load a new rules module based on blocking records:
   grep kesl /var/log/audit/audit.log | audit2allow -M kesl
   semodule -i kesl.pp
   ```

6. Switch SELinux to enforcing mode.

   ```
   setenforce Enforcing
   ```

How to create a Process start task

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux**.

   b. In the **Task type** drop-down list, select **Process start**.

   c. In the **Task name** field, enter a brief description.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option. Click **Next**.

5. Finish the wizard by clicking the **Finish** button.

   A new task will be displayed in the list of tasks.

6. Click the new task.

7. The task properties window opens.

8. Select the **Application settings** tab.

9. Enter the process start command:

   - **Executable command**. Field for entering the command to start the process.

     For example, if you want to run the `klnagchk` utility, which checks the connection to the Administration Server, `/opt/kaspersky/klnagent/bin/klnagchk`.

   - **Command line arguments (optional)**. Field for entering command line arguments to pass additional input to the script, utility, or application at startup.

     For example, you can enter the `-logfile /tmp/klnagchk.log` argument. This argument tells the tool to save the result to a file named `klnagchk.log` in `/tmp`. If you need to pass multiple arguments, separate them with spaces.

   - **Path to the working folder (optional)**. Field for entering the path to the working directory in which the process places the files.

     For example, you can enter `/tmp` and run the `klnagchk` utility with the following arguments: `-logfile klnagchk.log -savecert certificate.cer`. In this case, both files are created in `tmp`.

10. In the task properties window, select the **Schedule** tab.

11. Configure the task schedule.

12. Save your changes.

13. Select the check box next to the task.

14. Click **Start**.

As a result, Kaspersky Endpoint Security runs the command in silent mode and starts the process. You can view the results of the task in task properties in the **Execution results** section.

Terminate process

You can remotely terminate processes using the *Terminate process* task. For example, you can remotely terminate a process started as a result of malicious activity.

If you want to prohibit running a file, you can configure the Execution prevention component. You can prohibit the execution of executable files, scripts, office format files.

How to create a Terminate process task

1. In the main window of the Web Console, select **Tasks**.

   The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. Configure the task settings:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security for Linux**.

   b. In the **Task type** drop-down list, select *Terminate process*.

   c. In the **Task name** field, enter a brief description.

   d. In the **Devices to which the task will be assigned** block, select the task scope.

4. Select devices according to the selected task scope option. Click **Next**.

5. Finish the wizard by clicking the **Finish** button.

   A new task will be displayed in the list of tasks.

6. Click the new task.

7. The task properties window opens.

8. Select the **Application settings** tab.

9. To terminate the process, you must select the file of the process that you want to terminate. You can select a file in one of the following ways:

   - Enter the full name to the file.
   - Enter the hash of the file and the path to the file.
   - Enter the PID of the process (only for local tasks).
   - If the file is located on a network drive, enter the file path starting with `\\`, and not the drive letter. For example, `\\server\shared_folder\file.exe`. If the file path contains a network drive letter, you can get a *File not found* error.

10. In the task properties window, select the **Schedule** tab.

11. Configure the task schedule.

12. Save your changes.

13. Select the check box next to the task.

14. Click **Start**.

    As a result, Kaspersky Endpoint Security terminates the process on the computer. You can view the results of the task in task properties in the **Results** section.

Execution prevention for objects

You can apply this response action when integrating with Kaspersky Detection and Response solutions, from which Kaspersky Endpoint Security receives execution prevention rules.

If an object matches a rule, Kaspersky Endpoint Security prevents the execution of such an object.

Execution Prevention for objects EDR Expert (on-premises)

When integrating with Kaspersky Endpoint Detection and Response Expert (on-premise), Kaspersky Endpoint Detection and Response Expert (cloud), or Kaspersky Endpoint Detection and Response (KATA), you can configure rules to block the execution of objects in the console of the corresponding solution.

If integration with the Kaspersky Endpoint Detection and Response Expert (on-premises) solution or the Kaspersky Endpoint Detection and Response (KATA) component is enabled, you can enable or disable execution prevention for objects in the policy properties (**Application settings** → **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**).

To enable execution prevention for objects, set the toggle switch to **Execution Prevention ENABLED**.

Execution prevention for objects (EDR Optimum)

When integrated with Kaspersky Endpoint Detection and Response Optimum, you can configure Execution Prevention for objects and execution prevention rules in the Web Console.

How to enable execution prevention for objects in a Kaspersky Security Center policy

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.

5. Go to the **Execution Prevention** tab.

6. Set the toggle switch to **Execution Prevention ENABLED**.

7. Select an action on starting or opening an object

   - **Block and add to event log**. The application blocks the execution of objects or the opening of documents that satisfy the criteria of the prevention rules, and logs an event about attempts to run objects or open documents in the event log.

   - **Add to event log**. The application logs an event about attempts to run executable objects or open documents that satisfy the criteria of the prevention rules, but does not actually block their execution or opening.

8. Save your changes.

How to enable Execution Prevention for objects in the managed device properties

1. In the Web Console, go to **Asset management** → **Assets (Devices)**.

2. Click the link with the name of the device that you need.

3. This opens a selected device properties window; in that window, go to the **Applications** tab and click the <**Kaspersky Endpoint Security** application name> link.

   1. In the main window of the Web Console, select **Asset management** → **Policies**.

   2. Click the name of the Kaspersky Endpoint Security policy.

      The policy properties window opens.

   3. Select the **Application settings** tab.

   4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.

   5. Go to the **Execution Prevention** tab.

   6. Set the toggle switch to **Execution Prevention ENABLED**.

   7. Select an action on starting or opening an object

      - **Block and add to event log**. The application blocks the execution of objects or the opening of documents that satisfy the criteria of the prevention rules, and logs an event about attempts to run objects or open documents in the event log.

      - **Add to event log**. The application logs an event about attempts to run executable objects or open documents that satisfy the criteria of the prevention rules, but does not actually block their execution or opening.

   8. Save your changes.

4. Select the **Application settings** tab.

5. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.

6. Go to the **Execution Prevention** subsection.

7. Set the toggle switch to **Execution Prevention ENABLED**.

8. Select the mode of execution prevention for objects:

   - **Block**. In this mode, the application blocks the execution of objects or the opening of documents that satisfy the criteria of the prevention rules, and logs an event about attempts to run objects or open documents in the event log.

   - **Inform**. In this mode, the application logs an event about attempts to run executable objects or open documents that satisfy the criteria of the prevention rules in the event log, but does not actually block their execution or opening. This mode is selected by default.

9. Save your changes.

Object execution prevention cannot be enabled or disabled in the device properties if a policy is applied to the device.

How to add an Execution Prevention for objects rule of the EDR Optimum component in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. If necessary, select the **Use case-sensitive path** check box.

5. In the properties of the policy or the managed device, click the **Add** button in the toolbar above the list of execution prevention rules for objects.

6. This opens a window; in that window, enter the name of the execution prevention rule.

7. Specify the status of the execution prevention rule by setting the switch to the appropriate position.

8. In the **Type** drop-down list, select the type of object you want to block:

   - **Executable file**.

   - **Script**.

   - **Office application file**.

   If you select the wrong object type, the application will be unable to block the file or script.

9. To add an object, specify the path to the object and/or the checksum of the object (SHA256 or MD5 hash of the file) in the corresponding field.

10. Save your changes.

    The created rule is added to the list of rules in the **Execution prevention for objects** settings block.

Kaspersky Endpoint Security controls the execution of executable files and scripts, as well as the opening of office application files on the device. Execution prevention for objects supports a certain set of file extensions for office applications and a certain set of script interpreters. By blocking the launch of objects, you can stop the spread of a threat.

The execution prevention functionality is available in the Kaspersky Endpoint Security application if one of the following conditions is satisfied:

- Integration with the Kaspersky Endpoint Detection and Response Optimum is solution is enabled, and the EDR Optimum component is activated.
- Integration with the Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA) component is enabled, and the EDR Expert (on-premises) component is activated.
- Integration with the Kaspersky Endpoint Detection and Response Expert (cloud) is enabled, and the EDR Expert (cloud) component is activated.

If the blocking mode of file operation interception is not enabled, Execution Prevention for objects works in inform mode, regardless of the configured operating mode.

> Execution prevention for objects is disabled by default. Enabling execution prevention for objects may affect the startup speed of applications in the operating system.

For object execution prevention to work, you need to enable execution prevention rules.

Limitations and special considerations of execution prevention for objects

Limitations of execution prevention for objects

The following limitations apply to object execution prevention rules:

- The Kaspersky Endpoint Security application does not block objects specified in the execution prevention rules until the application is started.
- The Kaspersky Endpoint Security application does not block files that are opened before a prevention rule is created or modified.
- The Kaspersky Endpoint Security application does not block objects covered by an execution prevention rule that were executed before the execution prevention rule was created or modified to cover these objects.
- Some files can be critically important for the operation of the operating system and the application. Preventing the execution of such files may disrupt the operation of the system.

We do not recommend creating more than 50000 execution prevention rules because as this may lead to system instability.

Special considerations involved in object execution prevention when integrating with Kaspersky Endpoint Detection and Response Expert (on-premises) and Kaspersky Endpoint Detection and Response (KATA)

When the Kaspersky Endpoint Security application is integrated with the Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA), the application uses *execution prevention rules of the EDR Expert (on-premises) component*. The application gets these rules from Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA).

When integrated with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA), you can:

- Enable or disable the application of object execution prevention rules of the EDR Expert (on-premises) component in the Web Console or the Administration Console.

  When execution prevention rules are triggered, Kaspersky Endpoint Security sends a report to Endpoint Detection and Response Expert (on-premises) or Kaspersky Anti Targeted Attack Platform. For details, see the Help for the relevant solution.

- View the list of object execution prevention rules of the EDR Expert (on-premises) component on the command line.

Special considerations for Execution Prevention for objects when integrated with Kaspersky Endpoint Detection and Response Optimum

When Kaspersky Endpoint Security is integrated with the Kaspersky Endpoint Detection and Response Optimum solution, the application uses *object execution prevention rules of the EDR Optimum component*. You can create these rules manually in the Web Console. You can also create execution prevention rules automatically in the alert details window.

When integrated with Kaspersky Endpoint Detection and Response Optimum, you can:

- Enable or disable the application of object execution prevention rules of the EDR Optimum component in the Web Console.

- Create and configure EDR Optimum execution prevention rules for objects in the Web Console.

  You can also automatically create an execution prevention rule for an object by preventing the execution of a file in the alert details window. The execution prevention rule is added to the policy for the administration group that the device belongs to.

  > You can prevent the execution of files in the alert details window only if a policy is applied to the device.

- View the list of object execution prevention rules of the EDR Optimum component on the command line.

When integrated with Kaspersky Endpoint Detection and Response Optimum, object execution prevention can work in one of two modes:

- **Block**. In this mode, the application blocks the execution of objects or the opening of documents that satisfy the criteria of the prevention rules, and logs an event about attempts to run objects or open documents.

  > The Kaspersky Endpoint Security application blocks execution of a script that is prohibited by a run prevention rule, even if that script is imported by an allowed script.

- **Inform**. In this mode, the application logs an event about attempts to run executable objects or open documents that satisfy the criteria of the prevention rules, but does not actually block their execution or opening. This mode is selected by default.

Managing the Quarantine

Quarantine is a special storage location on the device for files that may be infected with viruses or cannot be disinfected at the time of detection. Quarantine allows isolating a file for further investigation. Quarantined files are stored in an encrypted form and do not threaten the security of the device. In contrast to Quarantine, Backup stores backup copies of files, in which malicious code was detected and which were deleted or modified during the disinfection process.

The application only uses Quarantine when integrated with Detection and Response solutions to perform recommended threat response actions. When the application is integrated with Kaspersky Endpoint Detection and Response Optimum or with Kaspersky Managed Detection and Response, you can also manually quarantine files that you consider dangerous for your device.

By default, the /var/opt/kaspersky/kesl/common/objects-backup/ directory is used to store quarantined files. This directory also contains Backup objects. You can change the directory for storing Backup and Quarantine objects using the command line.

Quarantined files may contain personal data. Root privileges are required to access quarantined files.

You can configure Quarantine settings on a device using a policy in the Web Console or in the Administration Console or using the command line. You can configure the following Quarantine settings:

- The percentage of Quarantine that must be full to generate an event about Quarantine being full. By default, an event is generated when the Quarantine is 90% full.
- Maximum size of the Quarantine in megabytes. When the maximum Quarantine size is reached, the application automatically deletes the oldest quarantined files. By default, the maximum Quarantine size is 200 MB if the application is being used in Standard mode or EDR Agent mode, and 100 MB if the application is being used in Light Agent mode.
- Path to the directory where Backup and Quarantine objects are stored (can only be configured on the command line).

How to manage Quarantine settings in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Reports and Storage**.
5. In the **Quarantine** section, configure the following settings:
   - **Limit the size of Quarantine**. Limiting Quarantine to the specified size in megabytes. This check box is selected by default.
   - **Maximum size of Quarantine (MB)**. If the **Limit the size of Quarantine** setting is enabled, you can specify the maximum size of Quarantine in megabytes (200 MB by default). The Quarantine size may not exceed 999,999 MB.

- **Notify when quarantine is full**. Notifications about the Quarantine becoming this percentage full. This check box is selected by default.

  You can specify the percentage after which a notification is sent (90% by default).

6. To apply the policy to computers, close the padlock icons and save your changes.

Quarantining files

Some files can be critically important for the operation of the operating system and the application. Quarantining such files can disrupt the operation of the system.

Placing a file in quarantine is possible only if one of the following conditions is met:

- Integration of Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Optimum is enabled and the EDR Optimum component is activated.
- Integration of the Kaspersky Endpoint Security application with the Kaspersky Endpoint Detection and Response Expert (on-premises) or Kaspersky Endpoint Detection and Response (KATA) component is enabled, and the EDR Expert (on-premises) component is activated.
- Integration of Kaspersky Endpoint Security with Kaspersky Managed Detection and Response is enabled and the MDR component is activated.

The directory for storing Quarantine objects must be writable.

When integrated with Kaspersky Endpoint Detection and Response (on-premises) or Kaspersky Endpoint Detection and Response (KATA), files can be quarantined in one of the following ways:

- By a task configured on the side of the Detection and Response solution. For details, see the Kaspersky Endpoint Detection and Response Expert (on-premises) Help or the Kaspersky Anti Targeted Attack Platform Help.
- As a result of executing the IOC Scan task on process memory.

When integrated with Kaspersky Managed Detection and Response, files are quarantined in one of the following ways:

- As a result of the execution of a task configured on the side of Kaspersky Managed Detection and Response.
- As a result of the execution of a command to manage the quarantine on the device.

For more information on working with Quarantine when integrated with Kaspersky Endpoint Detection and Response, see the Kaspersky Endpoint Detection and Response Help.

When integrated with Kaspersky Endpoint Detection and Response, files are quarantined in one of the following ways:

- Automatically as a result of the detection of indicators of compromise.
- As a result of a *Quarantine* task, which you can create in the Web Console.

- As a result of the execution of a command to manage the quarantine on the device.
- As a result of following the recommendation in the alert details.

For more information on managing the Quarantine when integrated with Kaspersky Endpoint Detection and Response Optimum, see the Kaspersky Endpoint Detection and Response Optimum Help.

Managing quarantined files

You can manage quarantined files:

- In Kaspersky Security Center, in the common list of files quarantined by Kaspersky applications.

  To manage quarantined files in Kaspersky Security Center, you need to enable the transfer of data about quarantined files to the Administration Server.

- Locally on the device using the command line.

You can view information about quarantined files, and delete and restore files from quarantine.

Restoring, deleting, and retrieving a file from Quarantine is available regardless of whether integration with Detection and Response solutions is enabled, and regardless of whether a policy is applied to the device.

The general list of files quarantined by Kaspersky applications on client devices is kept in Kaspersky Security Center and is available in the Administration Console (**Advanced** → **Repositories** → **Quarantine**) and the Web Console (**Operations** → **Repositories** → **Quarantine**). Kaspersky Security Center does not copy files from Quarantine storages to the Administration Server; all files are stored in Quarantine storages on client devices. For detailed information about managing quarantined files in Kaspersky Security Center, refer to the Kaspersky Security Center Help.

The quarantined file is restored to its original location according to the specified settings. Restoration preserves the MAC label (only on Astra Linux devices) and attributes of the original file (including the immutable and append-only attributes). A file with immutable and append-only attributes can only be restored to the location if the original file is not present, or to the original location, but with a different name. Root privileges are required to restore a file from Quarantine to a different directory or to the original location with a different name.

Once the restoration process is complete, the application deletes the quarantined copy of the restored file.

Restoring a file from quarantine fails in the following cases:

- The file to be restored was not found in the quarantine storage.
- The name of the file being restored is specified incorrectly or with the wrong case.
- The file ID was specified incorrectly.
- The destination directory has been deleted, moved, renamed, or you do not have access rights to it.

  In this case, the application moves the file to the /var/opt/kaspersky/kesl/common/restored/ directory. You can manually move the file from this directory to the directory of your choice.

- A file with the same name already exists at the specified path.

- The device does not have enough space.
- Only on Astra Linux devices: the MAC label of the file is higher than the MAC label of the directory into which the file is being restored.
- Only on Astra Linux devices: the MAC label of the file is lower the MAC label of the directory into which the file is being restored, and the ccnr flag is not set for this directory.

Deleting a file from quarantine fails in the following cases:

- The file to be deleted was not found in the quarantine storage.
- The name of the file being deleted is specified incorrectly or with the wrong case.
- The file ID was specified incorrectly.

Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum is a solution for protecting an organization's IT infrastructure from threats such as exploits, ransomware, fileless attacks, and legitimate system tools used by attackers to compromise devices or data.

Kaspersky Endpoint Security 12.5 for Linux is compatible with Kaspersky Endpoint Detection and Response Optimum version 3.1.

Integration of Kaspersky Endpoint Security with the Kaspersky Endpoint Detection and Response Optimum solution is facilitated by a Kaspersky Endpoint Security component: Endpoint Detection and Response Optimum (*EDR Optimum*).

For centralized management of the Kaspersky Endpoint Security application with the EDR Optimum component, use Kaspersky Security Center Windows 15.1 or Kaspersky Security Center Linux 15.3, 15.4, 16.0, 16.1, 16.2.

The component is not available for devices with an Elbrus CPU.

How Kaspersky Endpoint Detection and Response Optimum works

Kaspersky Endpoint Detection and Response Optimum monitors and analyzes the evolution of threats, and provides information about a potential attack to a security officer or administrator, helping them perform threat response actions in a timely manner.

Kaspersky Endpoint Detection and Response Optimum uses the following Threat Intelligence tools:

- The Kaspersky Security Network (hereinafter also referred to as KSN) cloud service infrastructure that provides access to Kaspersky file, website, and software reputation online knowledge base.
- Integration with the Kaspersky Threat Intelligence Portal, which contains and displays information about the reputation of files and websites.
- The Kaspersky Threats database.

When interacting with Kaspersky Endpoint Detection and Response Optimum, Kaspersky Endpoint Security can:

- Send data about events on devices to Kaspersky Security Center. Kaspersky Endpoint Security sends monitoring data on processes, open network connections, and modified files to Kaspersky Security Center, as well as data on threats detected by the application and data on the processing results for these threats.
- Perform threat response actions to maintain security when receiving commands from Kaspersky Security Center.

Configuring the Kaspersky Endpoint Detection and Response Optimum integration

Prerequisites

Before configuring the Kaspersky Endpoint Detection and Response Optimum integration:

- Add the EDR Optimum license key to the application if you have purchased a separate license to use this functionality.

  If you are using Kaspersky Endpoint Security under a license that includes Kaspersky Endpoint Detection and Response Optimum, no action is required.

  > If Kaspersky Endpoint Security is used in Light Agent mode, the license key is added to the SVM.

- Make sure the following is enabled and working:
  - Kaspersky Security Network in standard or extended mode:

    > For the most effective operation of Kaspersky Endpoint Detection and Response Optimum, we recommend the extended Kaspersky Security Network mode.

  - The following components of the Kaspersky Endpoint Security application:
    - File Threat Protection.
    - Behavior Detection.

  To make sure the telemetry is complete and to build a threat development chain in Kaspersky Security Center, you need to additionally enable Web Threat Protection.

  You can also enable execution prevention for objects.

Essential configuration steps

1. **Install the Kaspersky Endpoint Detection and Response Optimum management plug-in**

   The Kaspersky Endpoint Detection and Response Optimum management plug-in is a unified plug-in for managing agents on Windows, Mac, and Linux operating systems; the plug-in is necessary to display and view alert details. For a description of the installation procedure, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

   If your infrastructure uses the Kaspersky Security Center Cloud Console for managing Kaspersky Endpoint Detection and Response Optimum, the plug-in is installed by default.

2. **Configure the Kaspersky Endpoint Detection and Response Optimum integration settings**

   You can configure it:

   - Using the Web Console (Kaspersky Security Center Console and/or OSMP Console).
   - Using the command line.

   > Managing the EDR Optimum component using Kaspersky Security Center Administration Console is not supported.

3. **Enable data transfer to the Administration Server**

   To use all functionality of Kaspersky Endpoint Detection and Response Optimum, you must configure the following:

   - Enable sending information about files in Backup and Quarantine to the Kaspersky Security Center storage. To do this, you need to select the following check boxes in the policy properties:
     - **About files in Backup**
     - **About files in Quarantine**
   - Allow display of alert list To do this, you can enable the **Show EDR alerts** toggle switch in the main window of Kaspersky Security Center Web Console under **Settings** → **Interface settings**.

     > The **Show EDR alerts** setting not available in a Web Console version earlier than 15.1. You can navigate to EDR alerts from the Report on threats in the Kaspersky Security Center console.

   - Enable transmission of information about third-party application events on managed devices. To do this, run the following command on the managed device:

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     > Enabling this setting may significantly increase an operating system load.

4. **Make sure that the connection to Kaspersky Endpoint Detection and Response Optimum has been established successfully**

   Check the status of Kaspersky Endpoint Detection and Response Optimum in any convenient way.

The Kaspersky Endpoint Detection and Response Optimum integration is configured When a threat is detected, an alert is generated. In the alert details window, you can view information about the threat and perform response actions.

How to enable the EDR Optimum integration

In the Web Console, you can enable or disable the EDR Optimum component and configure the integration with Kaspersky Endpoint Detection and Response Optimum in the policy properties.

How to enable the Kaspersky Endpoint Detection and Response Optimum integration in the Web Console

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Enable the **Endpoint Detection and Response ENABLED** toggle switch.
6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to enable the Kaspersky Endpoint Detection and Response Optimum integration on the command line

To enable the EDR Optimum component, run the following command:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

1. In the main window of the Web Console, select the **Asset management** → **Assets (Devices)** section.
2. Click the link with the name of the device that you need.
3. This opens a selected device properties window; in that window, go to the **Applications** tab and click the <Kaspersky Endpoint Security application name> link.
4. Go to the **Application settings** tab, click the **Detection and Response** section, then click the **Endpoint Detection and Response Optimum** link.
5. This opens a window; in that window, set the toggle switch to **Endpoint Detection and Response Optimum Enabled** to enable the integration.
6. If necessary, manage the following settings:
   - Duration of device blocking as part of automatic network isolation.

     Click the **Configure device unblocking** link and specify the blocking time.
   - Automatic network isolation exclusions
7. Save your changes.

The managed device is configured for integration with Kaspersky Endpoint Detection and Response Optimum.

How to verify that the EDR Optimum integration is up and running

Read the information about possible integration statuses and when they may be displayed.

You can test the EDR Optimum component in the following ways:

- On the command line using the following command:

  ```
  kesl-control --app-info
  ```

  The EDR Optimum Integration is displayed with the **Running** status.

- In the Web Console:

  - Using the *Report on the status of application components*. For detailed information about reports, please refer to the Kaspersky Security Center Help.

  - Go to the **Asset management** → **Assets** section → <device name> link → **Applications** tab → <name of the Kaspersky Endpoint Security application> link → **General** tab → **Components**.

    The Endpoint Detection and Response Optimum component is displayed with the **Running** status.

Cloud Sandbox

Cloud Sandbox is a technology that lets you detect advanced threats on a computer. Kaspersky Endpoint Security automatically forwards detected files to Cloud Sandbox for analysis. Cloud Sandbox runs these files in an isolated environment to detect malicious activity and decides on the reputation of these files. Data on these files is then sent to Kaspersky Security Network. Therefore, if Cloud Sandbox has detected a malicious file, Kaspersky Endpoint Security will perform the appropriate action to eliminate this threat on all computers where this file is detected.

For Cloud Sandbox to operate, you must enable the use of Kaspersky Security Network.

If you are using Kaspersky Private Security Network, the Cloud Sandbox technology is not available.

The Cloud Sandbox technology is always enabled and is available to all users of Kaspersky Security Network, regardless of the type of license. If you have already deployed Endpoint Detection and Response Optimum solution, you can enable a separate counter for threats detected by Cloud Sandbox. You can use this counter to compile statistics when analyzing detected threats. Kaspersky Endpoint Security indicates the Cloud Sandbox threat detection technology in the *Report on threats* in the Kaspersky Security Center console.

How to enable the Cloud Sandbox counter in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response**.
5. Select the **Cloud Sandbox** tab.
6. Enable the **Cloud Sandbox ENABLED** toggle switch.
7. To apply the policy to computers, close the padlock icons and save your changes.

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Detection and Response Expert (on-premises) is an enterprise cyber security solution that allows defending against most cybersecurity risks and cover the main scenarios of threat spread. Components of Kaspersky Endpoint Detection and Response Expert (on-premises) are deployed on the Open Single Management Platform (OSMP). For more information about the solution and the platform, see the Kaspersky Endpoint Detection and Response Expert (on-premises) Help.

Integration with the Kaspersky Endpoint Detection and Response Expert (on-premises) solution is provided by the Kaspersky Endpoint Security application component, Endpoint Detection and Response Expert (on-premises) (hereinafter also referred to as *EDR Expert (on-premises)*).

The component is not available for devices with an Elbrus CPU.

How Endpoint Detection and Response Expert (on-premises) works

1. **Devices with Kaspersky Endpoint Security establish secure connections with the OSMP threat response action server and the OSMP telemetry collection server**
2. **Kaspersky Endpoint Security sends data to the telemetry collection server on the OSMP platform**

   The following information is transmitted:

   - Information about events on the device
   - Information about threats detected by the application
   - Information about the results of processing these threats
   - Monitoring data for processes, open network connections and modified files
3. **Kaspersky Endpoint Security performs threat response actions**

   Response actions are performed on command from the threat response action server on the OSMP platform.

Configuring Kaspersky Endpoint Detection and Response Expert (on-premises) integration

Prerequisites

Before configuring the integration with Kaspersky Endpoint Detection and Response Expert (on-premises):

- Allow connection on ports 443 and 8443.
- Enable the Behavior Detection component to transmit the necessary telemetry.

  If you want to get information about detected threats from other protection components, enable these components:

  - File Threat Protection.
  - Network Threat Protection.
  - Web Threat Protection.
  - Anti-Cryptor.
  - Application Control.
  - Device Control.
  - System Integrity Monitoring.

  > If Behavior Detection uses the eBPF mechanism to get system telemetry (available on 64-bit operating systems with kernel version 4.18 or later with eBPF support), the telemetry data is more comprehensive.

- Add the EDR Expert (on-premises) license key to the application if you have purchased a separate license to use this functionality.

  If you are using Kaspersky Endpoint Security under a license that includes Kaspersky Endpoint Detection and Response Expert (on-premises), no action is required.

  If the application is used in Light Agent mode, the EDR Expert (on-premises) license key is added to the SVM.

- Also, you need to configure a collector, a correlator, and a storage on the OSMP platform.

Essential configuration steps

1. **Get and process the certificates issued by the OSMP servers**

   When integrating with Kaspersky Endpoint Detection and Response Expert (on-premises), devices running Kaspersky Endpoint Security establish encrypted HTTPS connections with the OSMP threat response server and the OSMP telemetry server.

   > If the use of a proxy server is configured in the general settings of the Kaspersky Endpoint Security application, a proxy server is used for the connection to OSMP servers.

   Certificates for securing the connection with OSMP servers must be provided by the administrator of the OSMP platform.

To process certificates, follow the steps described in the Converting a PFX certificate to the PEM format article.

You can use a Server certificate and/or a Client certificate. The choice is determined by the security policy of your organization.

2. **Configure the Kaspersky Endpoint Detection and Response Expert (on-premises) integration settings**

   You can configure it:

   - Using the Web Console (Kaspersky Security Center Console and/or OSMP Console).
   - Using the command line.

   If you want to use Execution prevention for objects, you can enable the rules for execution prevention of objects of the EDR Expert (on-premises) component.

3. **Verify that the connection to the Endpoint Detection and Response Expert (on-premises) platform has been established successfully**

   Check the status of EDR Expert (on-premises) in any convenient way.

4. **Manage additional settings if necessary**

   - If SELinux is configured in Enforcing mode on your operating system, you will need to additionally configure SELinux to perform response actions.
   - To perform the **Memory dump** or **Process dump** response action, unblock ptrace.
   - Review the limitations of network isolation.
   - Enable transmission of information about third-party application events on managed devices. To do this, run the following command on the managed device:

     ```
     kesl-control --set-app-settings SystemEventsTransmission=Yes
     ```

     Enabling this setting may significantly increase an operating system load.

How to prepare a reference image for correct integration with EDR Expert (on-premises)

Before preparing the image, make sure that the `/var/opt/kaspersky/.ids_generated` file does not exist on the reference device.

To prepare a reference image for correct integration with Kaspersky Endpoint Detection and Response Expert (on-premises):

> Do not reboot the reference device or restart the Kaspersky Endpoint Security application while following these instructions.

1. Run the following commands as root:

```
systemctl stop kesl
systemctl edit kesl
```

2. In the editor, add one of the following configurations between the lines `### Anything between here and the comment below will become the contents of the drop-in file` and `### Edits below this comment will be discarded`:

   - Update the SensorID every time the application is started on temporary virtual machines

   ```
   [Service]
   ExecStartPre=-/usr/bin/uuid-regen.sh -a
   ```

   - Update the SensorID only once on persistent virtual machines

   ```
   [Service]
   ExecStartPre=-/usr/bin/uuid-regen.sh -b
   ```

3. Save your changes and close the editor.

   The `/etc/systemd/system/kesl.d/override.conf` file is created. Review its contents to make sure it matches the added configuration.

4. Reload the systemd service by running the following command:

```
systemctl daemon-reload
```

5. Create the `/usr/bin/uuid-regen.sh` file with the following content:

```
#!/usr/bin/env bash
# ------------------------------------------------------------
#  Kaspersky IDs updater
#  Modes:
#    -a   Always regenerate the IDs (default)
#    -b   Generate them only once – subsequent runs do nothing
#  Exit code: always 0
# ------------------------------------------------------------
set -euo pipefail
# ----- configuration ------------------------------------------------
PCID_FILE="/var/opt/kaspersky/kesl/common/pcid"
INSTALL_ID_FILE="/var/opt/kaspersky/epagent/install_id"
KESL_INI="/var/opt/kaspersky/kesl/common/kesl.ini"
# Marker that shows the script has already been executed in mode b
MARKER="/var/opt/kaspersky/.ids_generated"
# ----- default mode -------------------------------------------------
MODE="a"
# ----- parse command-line arguments ----------------------------------
while getopts ":ab" opt; do
   case $opt in
       a) MODE="a" ;;
       b) MODE="b" ;;
       \?) echo "Invalid option: -$OPTARG" >&2; exit 0 ;;
   esac
done
shift $((OPTIND-1))
# ----- helper: generate a new UUID and write to a file ---------------
write_uuid() {
   local target=$1
   /usr/bin/uuidgen > "$target"
}
# ----- helper: replace MachineId in kesl.ini -------------------------
replace_machine_id() {
   local new_id
   new_id=$(/usr/bin/uuidgen)
   /usr/bin/sed -i "s/^MachineId=.*/MachineId=${new_id}/" "$KESL_INI"
}
# ----- main logic ----------------------------------------------------
if [[ "$MODE" == "b" && -f "$MARKER" ]]; then
   # Mode b – already ran once → do nothing
   :
else
   # (re)generate all required values
   write_uuid "$PCID_FILE"
   write_uuid "$INSTALL_ID_FILE"
   replace_machine_id
   # In mode b remember that we have already executed
   if [[ "$MODE" == "b" ]]; then
       /usr/bin/touch "$MARKER"
   fi
fi
exit 0
```

6. Change the permissions of the `/usr/bin/uuid-regen.sh` file using the following command:

```
chmod 700 /usr/bin/uuid-regen.sh
```

The reference device is now ready for the creation of the operating system image.

How to configure the EDR Expert (on-premises) integration

In the Web Console, you can enable or disable the EDR Expert (on-premises) component and configure the integration of Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Expert (on-premises) in the Kaspersky Endpoint Security policy properties.

How to configure the Kaspersky Endpoint Detection and Response Expert (on-premises) integration in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.
5. Select the **Endpoint Detection and Response Expert version 8.0 or later** option.
6. Add telemetry collection servers and response servers.

   To do this, in the **Connection to telemetry collection servers** and **Connection to threat response servers** sections, click the **Add** button. In the window that opens, specify the server address (IPv4, IPv6) and the port to connect to the server.
7. Add certificates by clicking the **Connection settings** link in the **Connection to telemetry collection servers** and **Connection to threat response servers** sections; then in the displayed pane perform the following actions:

   a. Add a server certificate by clicking the **Upload** button in the corresponding section.

   b. If you need additional protection, create a crypto container.

      To do this, in the **Additional connection protection** section:

      1. Select the **Use two-way authentication** check box.
      2. Click the **Upload** button and add the client certificate you received when you completed the main integration scenario.
      3. Enter a password for the crypto container in the corresponding field.

      > The **Crypto container password** field is required. You cannot save the settings without entering a password for the client certificate (crypto container).
8. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to configure the Kaspersky Endpoint Detection and Response Expert (on-premises) integration on the command line

1. To add a response server certificate, run the following command:

   ```
   kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
   ```
2. To add a telemetry server certificate, run the following command:

   ```
   kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
   ```

3. To configure integration settings, run the following command:

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

The settings and their possible values are listed in the table below.

4. To add a client certificate for the connection to the response server, run the following command:

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
```

5. To add a client certificate for the connection to the telemetry server, run the following command:

```
kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
```

6. To enable integration with EDR Expert (on-premises), run the following command:

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response Expert (on-premises) Integration settings

Setting	Description	Value
`Mode`	Integration mode. For the Kaspersky Endpoint Detection and Response Expert (on-premises) integration, the Kaspersky Endpoint Security application interacts with servers on the OSMP platform. For the Kaspersky Endpoint Detection and Response (KATA) integration, the Kaspersky Endpoint Security application interacts with servers on the Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (default) is the EDR (KATA) integration mode. Allows enabling integration with Kaspersky Endpoint Detection and Response (KATA), a component of Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` is the EDR Expert (on-premises) integration mode. Enables the Kaspersky Endpoint Detection and Response Expert (on-premises) integration
`UseClientPinnedCertificate`	Enable or disable two-way authentication for additional security of the connection to the OSMP threat response action server. If two-way authentication is enabled on the OSMP threat response server side, you need to enable two-way authentication in the settings of *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task and add the client certificate before starting the task.	`Yes` enables two-way authentication for additional security of the connection to the OSMP threat response action server. `No` (default value) — do not use two-way authentication.
`SynchronizationPeriod`	Periodicity of synchronization requests to the OSMP threat response action server, in minutes.	Default value: `5`.
`ConnectionTimeout`	The maximum time to wait for a connection to the OSMP threat response action server, in seconds.	Default value: `10`.
`RequestTimeout`	The maximum time to wait for a response from the OSMP threat response action server, in seconds.	Default value: `10`.
`EnableTelemetry`	Sending data about events on devices (telemetry) to the OSMP telemetry collection server.	`Yes` (default value) enables the sending of telemetry to the OSMP telemetry server. `No` disables the sending of telemetry.
The **[Endpoints.item_#]** section contains the address and port of the OSMP threat response action server. You can add multiple servers.		

Setting	Description	Value
`Address`	OSMP threat response action server address. IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port for connecting to the OSMP threat response server.	Default value: `443`.
The **[TelemetrySettings]** section contains general settings for connecting to OSMP telemetry servers.		
`UseClientPinnedCertificate`	Enable or disable two-way authentication for additional security of the connection to the OSMP telemetry server. If two-way authentication is enabled on the OSMP telemetry server side, you need to enable two-way authentication in the settings of *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task and add the client certificate before starting the task.	`Yes` enables two-way authentication for additional security of the connection to the OSMP telemetry server. `No` (default value) — do not use two-way authentication.
`ConnectionTimeout`	The maximum time to wait for a connection to the OSMP telemetry server, in seconds.	Default value: `10`.
`RequestTimeout`	The maximum time to wait for a response from the OSMP telemetry server, in seconds.	Default value: `10`.
`OnlyTaggedEvents`	Sending telemetry with IOA only. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the *streaming scan* technology, which allows real time tracking of such events.	`Yes` – send only telemetry with an Indicator of Attack (IOA). `No` (default) – send all telemetry.
The **[TelemetrySettings.Endpoints.item_#]** section contains the address and port of the OSMP telemetry server. You can add multiple servers.		
`Address`	OSMP telemetry server certificate address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port for connecting to the OSMP telemetry server.	Default value: `443`.
The **[TelemetrySettings.EventTransferSettings]** section contains settings for data transfer to the OSMP telemetry server.		
`MaximumDataTransferTime`	The maximum delay in sending events to the OSMP telemetry server in seconds.	Default value: `30`.
`UseRequestCountLimits`	Limit the number of requests. This feature helps optimize the load on the server. If this functionality is enabled, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Endpoint Security stops sending events.	`Yes` (default value) – regulate the number of events sent. `No` – do not regulate the number of events.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	Default value: `3000`.
`MaximumNumberOfEventsInPackage`	Maximum number of events in one package.	Default value: `1024`.
`EventLimitExceededPercentage`	Number of events above the limit (percentage). Sending events is limited if the ratio of events of a certain type to the total number of events exceeds the configured threshold (as a percentage).	Default value: `15`.

For the settings of Kaspersky Endpoint Detection and Response Expert (on-premises) Integration, nested policies in the hierarchy allow specifying independent values, even if all other policy settings are inherited.

If Kaspersky Endpoint Detection and Response Expert (on-premises) Integration is enabled in the parent policy, and inheritance of settings is enabled in the child policy, then by default, the integration settings of the child policy are also inherited and cannot be changed. If you want to configure independent integration settings, select **Use custom connection settings** from the drop-down list. This makes Kaspersky Endpoint Detection and Response Expert (on-premises) Integration settings available for editing.

If you are using the Web Console or the command line, to integrate with Kaspersky Endpoint Detection and Response (on-premises), you need to select the EDR (on-premises) integration mode in the settings of the EDR Expert (on-premises) component:

- If you are using the Web Console, select **Endpoint Detection and Response Expert (version 8.0 or later)** in the policy settings. To configure integration with Kaspersky Endpoint Detection and Response (on-premises) on a device, in the Web Console, you need to manage the "padlocks" for either version (version 8.0 and later and version 7.1 and earlier).
- If you are using the command line, set `Mode=EDRExpertOnPrem` in the task settings.

How to verify that the EDR Expert (on-premises) Integration is up and running

How to test the EDR Expert (on-premises) component:

- On the command line using the following command:

  ```
  kesl-control --app-info
  ```

- In the Web Console.
  - In the Kaspersky Security Center Console:

    Using the *Report on the status of application components*. For detailed information about reports, please refer to the Kaspersky Security Center Help.
  - In the OSMP Console:
    - Using the *Report on the status of application components*.
    - Go to the **Asset management** → **Assets** section and select the **Analysis and response** tab.

      The device is displayed in the list with the **Normal activity** telemetry status.
    - Go to the **Threat hunting** section.

      Telemetry events from the device are displayed in the list of events.

Endpoint Detection and Response Expert (cloud)

Integration of Kaspersky Endpoint Security for Linux with Kaspersky Endpoint Detection and Response Expert (cloud) is temporarily unavailable. This functionality is planned to be supported by the end of 2026. Keep track of our Release Notes to be aware of application upgrades and new features.

Kaspersky Endpoint Security for Linux supports integration with the Kaspersky Endpoint Detection and Response Expert (cloud) solution. *Kaspersky Endpoint Detection and Response Expert (cloud)* is a cloud-based enterprise cybersecurity solution that includes Kaspersky applications that allow an organization to defend against most types of cyber risks and cover the most important threat propagation scenarios. EDR Expert (cloud) components are deployed on the Open Single Management Platform (OSMP). This platform runs cross-platform scenarios in a single interface and allows integrating Kaspersky applications with third-party applications into a comprehensive security system.

One of the central elements of the solution is *SIEM*. SIEM tracks events coming from all components and correlates these events with each other using vendor and user-defined rules. EDR Expert (cloud) looks at logs and telemetry received from the corporate infrastructure to automatically detect attacks and allows investigating incidents using a unified investigation graph which combines all events collected in EDR Expert (cloud), including events from Kaspersky applications and third-party information security products.

For response to advanced incidents, EDR Expert (cloud) uses preset and user-defined scenarios. You can also use response actions from third-party applications and response scenarios that involve multiple applications.

Threat Intelligence tools

Kaspersky Endpoint Detection and Response uses the following Threat Intelligence tools:

- Integration with Kaspersky Threat Intelligence Portal, which contains and displays information about the reputation of files and web addresses.
- The Kaspersky Threats database.
- The Kaspersky Security Network (hereinafter also referred to as "KSN") cloud service infrastructure, which provides access to real-time file, website, and software reputation information from the Kaspersky knowledge base. Using 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 positives.

Principle of operation of the solution

Kaspersky Endpoint Security is installed on individual computers on the corporate IT infrastructure and continuously monitors processes, open network connections, and files being modified.

Information about events on the computer (telemetry) is sent to the EDR Expert (cloud) server. In this case, Kaspersky Endpoint Security also sends information about threats discovered by the application as well as information about processing results for these threats to the telemetry collection servers.

The EDR Expert (cloud) integration is configured in the Kaspersky Security Center console. The built-in agent is then managed using the Open Single Management Platform (OSMP), including running tasks, managing quarantined objects, viewing reports, and other actions.

Limitations of EDR Expert (cloud)

- Kaspersky Endpoint Security does not support integration with EDR Expert (cloud) in Light Agent mode.
- EDR Expert (cloud) is not available for devices with an Elbrus CPU.
- EDR Expert (cloud) is not supported on devices based on the Arm architecture.
- EDR Expert (cloud) is not available for computers running 64-bit operating systems.

How to configure the built-in agent integration with EDR Expert (cloud)

To integrate with the Kaspersky Endpoint Detection and Response Expert (cloud) solution, you need to enable the Endpoint Detection and Response Expert (cloud) component and configure the connection to the telemetry collection server and the response server.

A *telemetry collection server* is a server that is part of a SIEM solution that collects, normalizes, correlates, analyzes, and stores information about events occurring on the computer.

A *response server* is a server for receiving and scanning data, studying the behavior of objects, and publishing the results of such studies.

> *Endpoint Detection and Response (cloud)* and *Endpoint Detection and Response Expert (on-premises)* components are not compatible with each other.

EDR Expert (cloud) operating conditions

For EDR Expert (cloud) to work, the following conditions must be met:

- The Kaspersky Endpoint Detection and Response Expert (cloud) infrastructure is available in your region. For information on the availability of the EDR Expert (cloud) infrastructure in your region, please contact Technical Support.
- OSMP (Open Single Management Platform) is installed.
- Kaspersky Endpoint Security installed in standard mode.
- The Kaspersky Endpoint Security application is activated and the functionality is covered by the license.
- You have accepted the terms of the Kaspersky Endpoint Detection and Response Expert (cloud) Data Processing Agreement.
- The Endpoint Detection and Response Expert (cloud) component is enabled.
- The Behavior Detection component for transmitting the necessary telemetry is enabled.

If you want to get information about detected threats from other protection components, enable these components:

- File Threat Protection.
- Network Threat Protection.
- Web Threat Protection.
- Anti-Cryptor.
- Application Control.
- Device Control.
- System Integrity Monitoring.

Steps for integrating with EDR Expert (cloud)

Setting up EDR Expert (cloud) Integration involves the following steps:

1. **Selecting an EDR Expert mode**

   Kaspersky Endpoint Security supports two EDR Expert modes: on-premises and cloud. To integrate with Kaspersky Endpoint Detection and Response Expert (cloud), you need to enable the corresponding mode during installation of the application. By default, the application uses the Endpoint Detection and Response Expert (on-premises) integration.

2. **Activating Kaspersky Endpoint Detection and Response Expert (cloud)**

   You need to purchase a separate license for Kaspersky Endpoint Detection and Response Expert (cloud).

   The functionality becomes available after adding a separate key for Kaspersky Endpoint Detection and Response Expert (cloud). As a result, two keys are added on the computer: a key for Kaspersky Endpoint Security and a key for Kaspersky Endpoint Detection and Response Expert (cloud).

   Licensing for the stand-alone Endpoint Detection and Response Expert (cloud) functionality is the same as the licensing of Kaspersky Endpoint Security.

   Make sure that EDR Expert (cloud) functionality is covered by your license and works in Kaspersky Security Center or on the protected device.

3. **Configuring the connection to the telemetry collection server and response server**

   Kaspersky Endpoint Detection and Response Expert (cloud) requires a trusted connection between Kaspersky Endpoint Security and two servers: the telemetry collection server and the response server. The application receives server addresses and certificates for establishing a trusted connection automatically after you accept the terms and conditions of the Kaspersky Endpoint Detection and Response Expert (cloud) agreement on data processing. Thus, you only need to manage advanced settings for connecting to servers: whether you want to use a TCP tunnel and the period for sending a request to synchronize with the server.

How to configure additional settings for connecting Kaspersky Endpoint Security to EDR Expert (cloud) in the Web Console

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
5. Enable the component using the **Endpoint Detection and Response Expert (cloud) DISABLED** toggle switch.
6. If the current policy is a child policy and the parent policy prohibits changes to the EDR Expert (cloud) integration settings (closed "padlock"), you can configure setting inheritance in the **Inheritance** section:
   - **Inherit connection settings from the policy** (default value). The connection settings will be inherited from the parent policy. You will not be able to edit the settings.
   - **Use custom connection settings**. You can configure the connection settings manually.
7. The **Response server** tab displays the fully qualified domain name and port of the response server, which are retrieved automatically. If the security policy in your infrastructure does not allow you to connect directly to EDR Expert (cloud) servers, you can set up a connection via a TCP tunnel:

   a. Select the **Use a TCP tunnel for response** check box.

   b. Specify the server address (IPv4, IPv6) and the port to connect to the tunnel.
8. If necessary, set the frequency of sending synchronization requests to the server in the **Send sync request to server every (min)** field. During the synchronization, Kaspersky Endpoint Security receives threat response tasks and sends task results.
9. Go to the **Telemetry collection server** tab.
10. Configure the telemetry collection server connection settings:

    a. Click the **Edit** link.

    b. This opens a window; in that window, select a telemetry collection server from the list. The KUMA collector serves as the telemetry collection server in EDR Expert (cloud). For more details, please refer to the Kaspersky Unified Monitoring and Analysis Platform Help.

    If an error occurs while connecting to the telemetry collection server, select a different server. If you are unable to connect to the telemetry collection server, please contact Technical Support.

    c. If necessary, you can configure a connection to the telemetry collection server via a TCP tunnel, just as you would for the response server.
11. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to view certificate information on the command line

1. To view information about a client certificate, run the following command:

```
kesl-control --query-cloudxdr-client-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-client-certificate --server-type response
```

2. To view information about a server certificate, run the following command:

```
kesl-control --query-cloudxdr-server-certificate --server-type telemetry
```

```
kesl-control --query-cloudxdr-server-certificate --server-type response
```

As a result, Kaspersky Endpoint Security will display the certificate information as follows:

```
Serial number: 12 34 56 78 AB CD EF GH
Subject: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Issuer: C=EN, ST=Moscow, L=Moscow, O=AO Kaspersky Lab, OU=Future Technologies, CN=epp
Valid from: 2022-07-27 13:25:35
Expires on: 2072-07-14 13:25:35
SHA1 fingerprint: a14f12df23fg3465bgh6345g567df
```

Check the operating status of the component by viewing the *Report on status of application components*. You can also view the status of the component on the protected device.

How to optimize EDR Expert (cloud) telemetry transmission

Telemetry is a list of events that have occurred on the protected computer. Kaspersky Endpoint Security analyzes telemetry data and sends it to telemetry collection servers during synchronization. Telemetry events arrive on the server almost continuously. Kaspersky Endpoint Security initiates synchronization with the server when any of the following conditions are satisfied:

- Synchronization interval has run out.
- The number of events in the buffer exceeds the upper limit.

Therefore, by default, the application synchronizes every 30 seconds or whenever the buffer holds 1024 events. You can configure the synchronization behavior in the Kaspersky Endpoint Security policy and select optimum values to match your network load (see instructions below).

If there is no connection between Kaspersky Endpoint Security and the server, the application queues new events. When the connection is restored, Kaspersky Endpoint Security sends queued events to the server in proper order. To avoid overloading the server, Kaspersky Endpoint Security may skip some events. To enable this, you can optimize event transmission settings, for example, to set a maximum events-per-hour value (see instructions below).

How to optimize telemetry transmission in the Web Console

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (cloud)**.
5. In the window that opens, select the **Data transmission settings** tab.
6. Make sure the **Sending telemetry ENABLED** check box is selected.
7. If required, enable the **Send telemetry with IOA only** functionality. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the *streaming scan* technology, which allows real time tracking of such events. The function is disabled by default.
8. If necessary, configure the server synchronization settings:
   - **Maximum event transmission delay (sec)**. The application synchronizes with the server to send events after the synchronization interval expires. The default setting is 30 seconds.
   - **Maximum number of event packages**. The application synchronizes with the server when the buffer is filled with events. The default setting is 1024 events.
9. Go to the **Request throttling** tab.
10. If necessary, disable request throttling using the **Request throttling ENABLED** toggle switch.

    This feature helps optimize the load on the server. If this functionality is enabled, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Endpoint Security stops sending events. This option is disabled by default.
11. Configure optimization settings for sending events to the server:
    - **Maximum number of events per hour**. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Endpoint Security resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.
    - **Percentage of event limit excess (%)**. The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Endpoint Security resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.
12. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to optimize telemetry transmission on the command line

1. To enable the sending of telemetry, run the following command:

```
kesl-control --set-settings 39 [EnableTelemetry=<Yes|No>] [TelemetrySettings.OnlyTaggedEvents=<Yes|No>]
```

2. To configure synchronization settings with the server, run the following command:

```
kesl-control --set-settings 39 [TelemetrySettings.EventTransferSettings.UseRequestCountLimits=<Yes|No>]
[TelemetrySettings.EventTransferSettings.MaximumDataTransferTime=<delay in sending events in seconds>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInHour=<number of events>]
[TelemetrySettings.EventTransferSettings.MaximumNumberOfEventsInPackage=<number of event packages>]
[TelemetrySettings.EventTransferSettings.EventLimitExceededPercentage=<percentage of exceeding the event
limit>]
```

Kaspersky Endpoint Detection and Response Expert (cloud) integration settings

Setting	Description
`EnableTelemetry`	Sending data about events on devices (telemetry) to the OSMP telemetry collection server. Sending telemetry is enabled by default (`Yes`).
`TelemetrySettings.OnlyTaggedEvents`	Sending telemetry with IOA only. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the *streaming scan* technology, which allows real time tracking of such events. By default, sending telemetry with IOA only is disabled (`No`).
The `[TelemetrySettings.EventTransferSettings]` section contains general settings for connecting to OSMP telemetry servers.	
`UseRequestCountLimits`	Request throttling. This feature helps optimize the load on the server. If this functionality is enabled, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Endpoint Security stops sending events. This option is disabled by default.
`MaximumDataTransferTime`	Maximum event transmission delay (sec). The application synchronizes with the server to send events after the synchronization interval expires. The default setting is 30 seconds.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour. The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Endpoint Security resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.
`MaximumNumberOfEventsInPackage`	Maximum number of events in package. The application synchronizes with the server when the buffer is filled with events. The default setting is 1024 events.
`EventLimitExceededPercentage`	Percentage of event limit excess (%). The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Endpoint Security resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.

How to configure EDR Expert (cloud) telemetry exclusions

To improve performance and optimize data transmission to the telemetry collection server, you can add telemetry exclusions. For example, you can choose not to send network communications data for individual applications.

Using too many rules can increase the load on the Telemetry collection server and reduce the computer performance. We recommend adding only necessary rules.

To create a telemetry exclusion in the Web Console:

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.
   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Telemetry Settings**.
5. Select the **EDR Expert (cloud) telemetry** tab.
6. In the **General exclusions** block, click the **Add** button.
   This opens a window for adding a telemetry exclusion rule.
7. Configure the telemetry exclusion rule:

   a. If necessary, change the status of the rule. By default, the rule is enabled.

   b. Enter a name for the rule.

   c. Select the action to be performed when the rule is triggered:

   - **Do not collect**. The filtered event will be excluded from the sent telemetry.
   - **Exclude IOA**. The IOA rule trigger event will be excluded from the sent telemetry. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the *streaming scan* technology, which allows real time tracking of such events.

   d. If the **Exclude IOA** option is selected, specify the IOA rules to be added to exclusions:

   - **Exclude all**. When the specified condition is met, the application will exclude events generated based on all IOA rules from the telemetry.
   - **Exclude by GUID**. Specify the GUID of the IOA rule. You can specify multiple GUIDs by using `,`. For more details on the IOA rules, please refer to the EDR Expert (cloud) Help.

   e. Specify the filtering conditions:

   If necessary, you can create complex filter criteria by adding multiple filter conditions and groups of conditions using the **AND**, **OR**, and **NOT** operators. You can also add nested conditions and condition groups to a condition group.

8. If necessary, under **All event types**, add telemetry exclusions by event type.

   a. Click the event type name.

   b. In the window that opens, click the **Set up manually** button.

c. In the **Exclusion rules** block, click the **Add** button.

This opens a window for adding a telemetry exclusion rule. In the telemetry exclusion rule, the `EventType` filtering condition is already preset in the rule, which corresponds to the type of event.

d. Specify the filtering conditions:

9. To apply the policy to computers, make sure that the padlocks are closed (🔒) and save your changes.

How to export or import EDR Expert (cloud) event filters

You can export the list of exclusions to a JSON file. Then you can modify the file to, for example, add a large number of event IDs. You can also use the export/import function to back up the event filters or to migrate the list to a different server.

> Using too many rules can increase the load on the Telemetry collection server and reduce the computer performance. We recommend adding only necessary rules.

To export or import event filters in the Web Console:

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Telemetry Settings**.
5. Select the **EDR Expert (cloud) telemetry** tab.
6. To export the event filters:

   a. Click **Export**.

   b. In the window that opens, specify the name of the JSON file to which you want to export the event filters, and select the folder in which you want to save this file.

   c. Save the file.

   Kaspersky Endpoint Security exports the event filters to the JSON file.
7. To import the event filters:

   a. Click **Import**.

   b. In the window that opens, select the JSON file from which you want to import the event filters.

   c. Select how you want event filtering rules to be imported: by adding to existing rules or by discarding existing rules and replacing with new ones.

   d. Open the file.

8. To apply the policy to computers, make sure that the padlocks are closed (🔒) and save your changes.

1. In the main window of the Web Console, select the **Asset management** → **Policies** tab.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **General Settings** → **Telemetry Settings**.
5. Select the **EDR Expert (cloud) telemetry** tab.
6. To export the event filters:

   a. Click **Export**.

   b. In the window that opens, specify the name of the JSON file to which you want to export the event filters, and select the folder in which you want to save this file.

   c. Save the file.

   Kaspersky Endpoint Security exports the event filters to the JSON file.
7. To import the event filters:

   a. Click **Import**.

   b. In the window that opens, select the JSON file from which you want to import the event filters.

   c. Select how you want event filtering rules to be imported: by adding to existing rules or by discarding existing rules and replacing with new ones.

   d. Open the file.
8. To apply the policy to computers, make sure that the padlocks are closed (🔒) and save your changes.

Kaspersky Anti Targeted Attack Platform

Kaspersky Anti Targeted Attack Platform is a solution for protection of an organization's IT infrastructure and early detection of threats such as zero-day attacks, targeted attacks, and advanced persistent threats (hereinafter also referred to as APT). For details about the solution, please refer to the Kaspersky Anti Targeted Attack Platform Help.

The Kaspersky Endpoint Security application can integrate with the following components on the Kaspersky Anti Targeted Attack Platform:

Kaspersky Endpoint Detection and Response (KATA)

The component protects devices in the local network of an organization. When integrated with Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security performs the following functions:

- Sends information about events on devices (telemetry) to the Central Node server that provides interaction with Kaspersky Endpoint Detection and Response (KATA) (hereinafter also referred to as the *KATA server*).

  Kaspersky Endpoint Security sends monitoring data on processes, open network connections, and modified files to the Central Node component, as well as data on threats detected by the application and data on the results of processing these threats.

- Executes threat response actions to ensure security when receiving commands from Kaspersky Anti Targeted Attack Platform.

Integration with Kaspersky Endpoint Detection and Response (KATA) 7.1 and earlier is supported.

Network Detection and Response (KATA)

The component protects the internal network of an organization. When integrated with Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Security can send information about events on devices (telemetry) to the Central Node server that provides interaction with Kaspersky Network Detection and Response (KATA) (hereinafter also referred to as the *NDR server*).

Sandbox

The Kaspersky Endpoint Security application sends files for scanning to the Central Node server that handles the interaction with Sandbox.

The following components of Kaspersky Endpoint Security enable integration with Kaspersky Anti Targeted Attack Platform:

- Endpoint Detection and Response Expert (on-premises), hereinafter also referred to as *EDR Expert (on-premises)*.

  Starting with Kaspersky Endpoint Security 12.4 for Linux, the Endpoint Detection and Response (KATA) component has been renamed to Endpoint Detection and Response Expert (on-premises). Now this component provides integration not only with Kaspersky Endpoint Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform, but also with the Kaspersky Endpoint Detection and Response Expert (on-premises) solution.

- Network Detection and Response (KATA), hereinafter also *NDR (KATA)*.

- Sandbox.

You can configure the integration of the Kaspersky Endpoint Security application with all components of the Kaspersky Anti Targeted Attack Platform solution, as well as with each component individually.

The component is not available for devices with an Elbrus CPU.

Configuring the Kaspersky Anti Targeted Attack Platform integration

Prerequisites

Before configuring Kaspersky Network Detection and Response (KATA) Integration, allow connection on port 8085.

Before configuring the integration with the Kaspersky Endpoint Detection and Response (KATA) component:

- Allow connection on ports 443, 8443.
- Enable the Behavior Detection component to transmit the necessary telemetry.

  > The Behavior Analysis component is available on devices with kernel version 3.13 and later.

  If you want to get information about detected threats from other protection components, enable these components:

  - File Threat Protection.
  - Network Threat Protection.
  - Web Threat Protection.
  - Anti-Cryptor.
  - Application Control.
  - Device Control.
  - System Integrity Monitoring.

  Enabling eBPF network traffic interception mode makes telemetry data more comprehensive. The eBPF technology is available on computers running 64-bit operating systems with kernel version 4.18 or later with eBPF support.

  > We recommend checking if your computer supports the components that are required for sending telemetry.

- Add the EDR Expert (on-premises) license key to the application if you have purchased a separate license to use this functionality.

  If you are using Kaspersky Endpoint Security under a license that includes Kaspersky Endpoint Detection and Response Expert (on-premises), no action is required.

  > If you are using Kaspersky Endpoint Security in Light Agent mode, you need to add the license key for activating the additional functionality to SVMs.

Essential configuration steps

1. **Get and process the certificates issued by the Central Node servers**

While integrated with Kaspersky Anti Targeted Attack Platform, devices running Kaspersky Endpoint Security establish encrypted HTTPS connections with Central Node servers that provide the integration.

> If the general settings of Kaspersky Endpoint Security stipulate that a proxy server must be used, the connection to servers that handle the interaction with Kaspersky Anti Targeted Attack Platform components is made through a proxy server.

The certificates for securing the connections to servers that handle the interaction with components of the Kaspersky Anti Targeted Attack Platform solution must be provided by the Kaspersky Anti Targeted Attack Platform administrator.

To process certificates, follow the steps described in the Converting a PFX certificate to the PEM format article.

You can use a Server certificate and/or a Client certificate. The choice is determined by the security policy of your organization.

2. **Configure the Kaspersky Anti Targeted Attack Platform integration settings**

   You can configure it:

   - Using the Web Console (EDR (KATA) and NDR (KATA) in the Kaspersky Security Center console and/or the OSMP Console).
   - Using the Kaspersky Security Center Administration Console (EDR (KATA) and NDR (KATA)).
   - Using the command line (EDR (KATA) and NDR (KATA)).

3. **Verify that the connection to Kaspersky Anti Targeted Attack Platform has been successfully established.**

   Check the status of Kaspersky Anti Targeted Attack Platform components in any convenient way.

4. **Manage additional settings if necessary**

   - If SELinux is configured in Enforcing mode on your operating system, you will need to additionally configure SELinux to perform response actions.
   - Review the limitations of network isolation.

How to configure the EDR (KATA) integration

In the Web Console, you can enable or disable the Kaspersky Endpoint Detection and Response (KATA) component, and configure the integration of the Kaspersky Endpoint Security application with this component.

How to configure the Kaspersky Endpoint Detection and Response (KATA) integration in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. In the policy properties window that opens, select the **Application settings** tab.
5. Go to **Built-in Agents Configuration** → **Endpoint Detection and Response Expert (on-premises)**.

6. In the right part of the screen:

   a. Select the **Endpoint Detection and Response Expert version 7.1 or earlier** option.

   b. In the **Connection to telemetry collection servers** section, select a telemetry collection server by clicking the **Add** button in the toolbar, then click **Select server**.

   c. In the **Connection to response servers** section, select a response server by clicking the **Add** button in the toolbar, then click **Select server**.

   d. Click the **Connection settings** link in the **Connection to telemetry collection servers** and **Connection to threat response servers** sections, then in the displayed pane:

      1. Add a server certificate by clicking the **Upload** button.

      2. If you need additional protection, create a crypto container.

         To do this, in the **Additional connection protection** section:

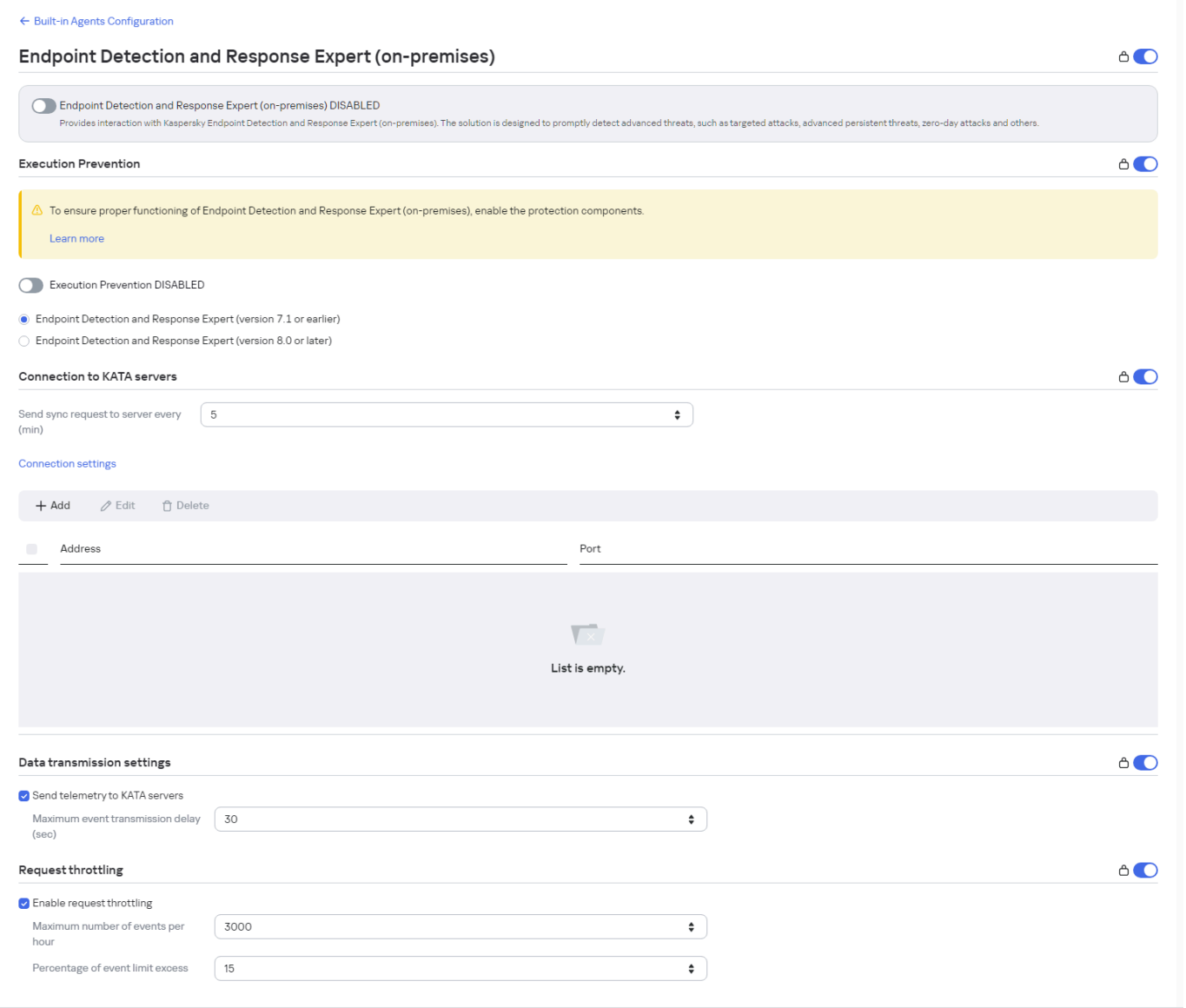
         - Select the **Use two-way authentication** check box.

         - Click the **Upload** button and add the client certificate that you obtained at step 1 of the main scenario.

         - Enter a password for the crypto container in the corresponding field.

         > The **Crypto container password** field is required. You cannot save the settings without entering a password for the client certificate (crypto container).

7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Endpoint Detection and Response Expert (on-premises)

How to configure the Kaspersky Endpoint Detection and Response (KATA) integration on the command line

1. To select an EDR (KATA) integration mode, run the following command:

```
kesl-control --set-settings 24 Mode=EDRKATA
```

2. To add a Central Node server, run the following command:

```
kesl-control --set-settings 24 Endpoints.item_001.Address=<central node server address>
Endpoints.item_001.Port=<central node server port>
```

3. To add a response server certificate, run the following command:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

4. To configure integration settings, run the following command:

```
kesl-control --set-settings 24 [<setting name>=<setting value>]
```

The settings and their possible values are listed in the table below.

5. To add a client certificate for the connection to the response server, run the following command:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

6. To enable integration with EDR (KATA), run the following command:

```
kesl-control --start-task 24
```

Kaspersky Endpoint Detection and Response (KATA) integration settings

Setting	Description	Value
`Mode`	Integration mode. For the Kaspersky Endpoint Detection and Response Expert (on-premises) integration, the Kaspersky Endpoint Security application interacts with servers on the OSMP platform. For the Kaspersky Endpoint Detection and Response (KATA) integration, the Kaspersky Endpoint Security application interacts with servers on the Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (default) is the EDR (KATA) integration mode. Allows enabling integration with Kaspersky Endpoint Detection and Response (KATA), a component of Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` is the EDR Expert (on-premises) integration mode. Enables the Kaspersky Endpoint Detection and Response Expert (on-premises) integration
`UseClientPinnedCertificate`	Enable and disable two-way authentication to further secure the connection to the KATA server. If two-way authentication is enabled on the KATA server side, you need to enable two-way authentication in the settings of *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task and add the client certificate before starting the task.	`Yes` – use two-way authentication to further secure the connection to the KATA server. `No` (default value) — do not use two-way authentication.
`SynchronizationPeriod`	Frequency of sending synchronization requests to the KATA server in minutes.	Default value: `5`.
`ConnectionTimeout`	Maximum time to wait for a connection to the KATA server in seconds.	Default value: `10`.
`RequestTimeout`	Maximum time to wait for a response from the KATA server in seconds.	Default value: `10`.
`EnableTelemetry`	Sending event data (telemetry) to KATA.	`Yes` (default value) – send telemetry to the KATA server. `No` disables the sending of telemetry.
The **[Endpoints.item_#]** section contains the address and port of the KATA server. You can add multiple servers.		
`Address`	KATA server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port to connect to the KATA server.	Default value: `443`.
The **[EventTransferSettings]** section contains settings for sending data to the KATA server.		
`MaximumDataTransferTime`	The maximum delay in sending events to the KATA server in seconds.	Default value: `30`.

Setting	Description	Value
`UseRequestCountLimits`	Enable and disable regulating the number of events sent to the KATA server.	`Yes` (default value) – regulate the number of events sent. `No` – do not regulate the number of events.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	Default value: `3000`.
`MaximumNumberOfEventsInPackage`	Maximum number of events in one package.	Default value: `1024`.
`EventLimitExceededPercentage`	Number of events above the limit (percentage). Sending events is limited if the ratio of events of a certain type to the total number of events exceeds the configured threshold (as a percentage).	Default value: `15`.

If you are using the Web Console or the command line, to integrate with Kaspersky Endpoint Detection and Response (KATA), you need to select the *EDR (KATA)* integration mode in the settings of the EDR Expert (on-premises) component:

- If you are using the Web Console, in the policy settings, select the **Endpoint Detection and Response Expert (version 7.1 or earlier)** option. To configure integration with Kaspersky Endpoint Detection and Response (KATA) on a device, in the Web Console, you need to manage the "padlocks" for either version (version 8.0 and later and version 7.1 and earlier).
- If you are using the command line, set `Mode=EDRKATA` in the task settings.

How to configure the NDR (KATA) integration

In the Web Console, you can enable or disable the Kaspersky Network Detection and Response (KATA) component, and configure the integration of the Kaspersky Endpoint Security application with this component.

How to configure the Kaspersky Network Detection and Response (KATA) integration in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Network Detection and Response (KATA)**.
5. Enable the **Network Detection and Response (KATA)** toggle switch.
6. Click **Connection settings**.
7. Configure the server connection:
   - **Timeout (sec)**. Maximum Central Node server response timeout. When the timeout runs out, Kaspersky Endpoint Security tries to connect to a different Central Node server.
   - **Server certificate**. TLS certificate for establishing a trusted connection with the Central Node server. You can get a TLS certificate in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help).

- **Use two-way authentication**. Two-way authentication when establishing a secure connection between Kaspersky Endpoint Security and the Central Node server. To use two-way authentication, you need to enable two-way authentication in the Central Node server settings, then get a crypto-container and set a password to protect the crypto-container. A *crypto-container* is a PFX archive with a certificate and a private key. You can get a crypto-container in the Kaspersky Anti Targeted Attack Platform console (see instructions in the Kaspersky Anti Targeted Attack Platform Help). After configuring the Central Node settings, you need to also enable two-way authentication in Kaspersky Endpoint Security settings and load a password-protected crypto-container.

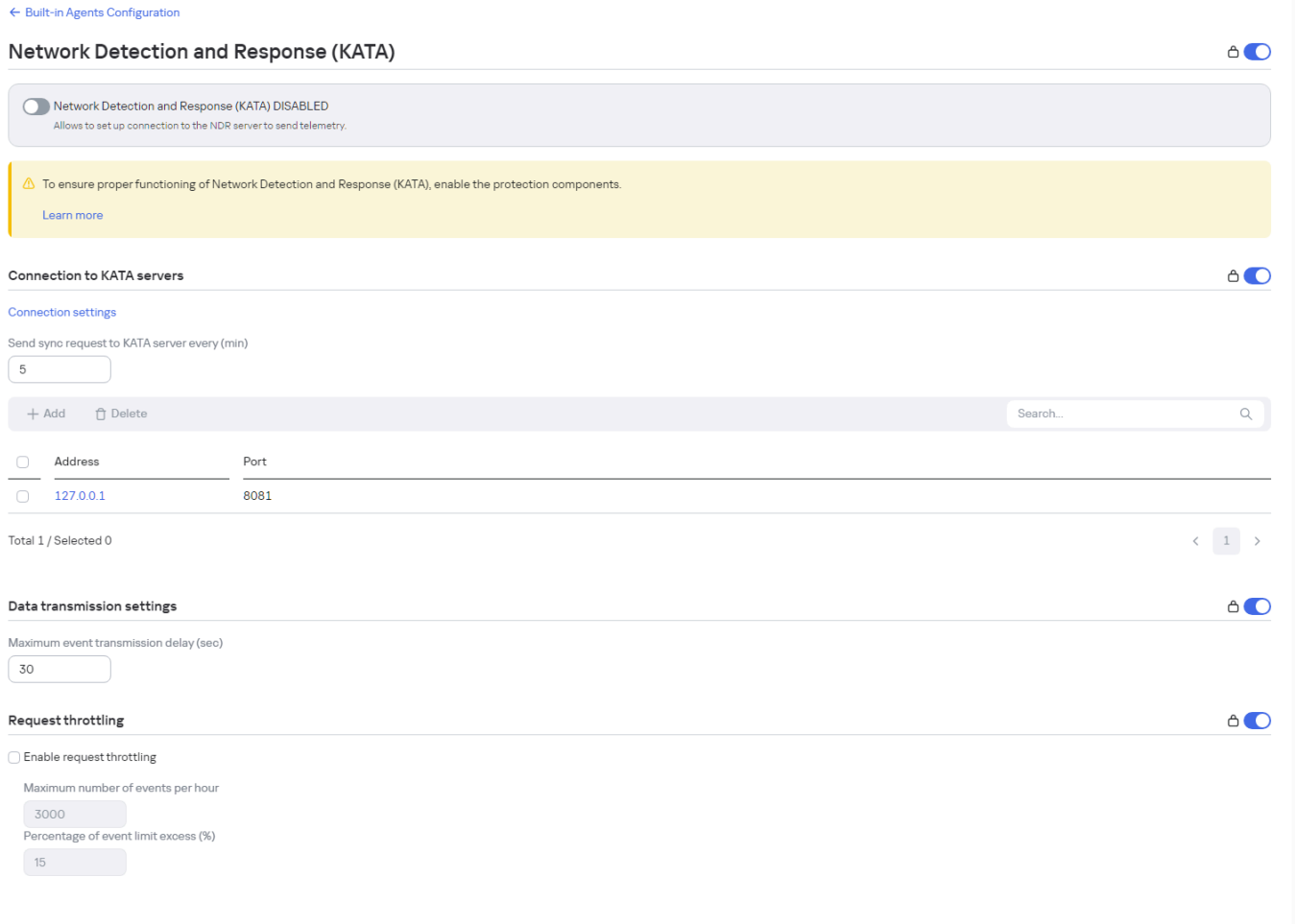
> The crypto-container must be password-protected. It is not possible to add a crypto-container with a blank password.

8. Click **OK**.

9. Add Central Node servers. To do this, specify the server address (IPv4, IPv6) and the port to connect to the server.

10. You can add multiple Central Node server addresses. Kaspersky Endpoint Security attempts to connect to the server using the first IP address. If a connection cannot be established, Kaspersky Endpoint Security tries to connect using the second IP address in the list and so on.

11. To apply the policy to computers, close the padlock icons and save your changes.



Network Detection and Response (KATA)

How to configure the Kaspersky Network Detection and Response (KATA) integration on the command line

1. To add a Central Node server, run the following command:

```
kesl-control --set-settings 31 Endpoints.item_001.Address=<cenral node server address> Endpoints.item_001.Port=
<central node server port>
```

2. To add a response server certificate, run the following command:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

3. To configure integration settings, run the following command:

```
kesl-control --set-settings 31 [<setting name>=<setting value>]
```

The settings and their possible values are listed in the table below.

4. To add a client certificate for the connection to the response server, run the following command:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

5. To enable integration with NDR (KATA), run the following command:

```
kesl-control --start-task 31
```

Kaspersky Network Detection and Response (KATA) Integration task settings

Setting	Description	Value
`UseClientPinnedCertificate`	Enable and disable two-way authentication to further secure the connection to the NDR server. If client certificate validation is enabled on the NDR server side, enable the use of a client certificate and add a client certificate before starting the *Kaspersky Network Detection and Response (KATA) Integration* task.	`Yes` – use two-way authentication to further secure the connection to the NDR server. `No` (default value) — do not use two-way authentication.
`SynchronizationPeriod`	Frequency of sending synchronization requests to the NDR server in minutes.	Default value: `5`.
`ConnectionTimeout`	Maximum time to wait for a connection to the NDR server in seconds.	Default value: `10`.
`RequestTimeout`	Maximum time to wait for a response from the NDR server in seconds.	Default value: `10`.
The **[Endpoints.item_#]** section contains the address and port of the NDR server.		
`Address`	NDR server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified.	Default value: `127.0.0.1`.
`Port`	Port to connect to the NDR server.	Default value: `8081`.
The **[EventTransferSettings]** section contains settings for sending events to the NDR server.		
`MaximumDataTransferTime`	The maximum delay in sending events to the NDR server in seconds.	Default value: `30`.
`MaximumNumberOfEventsInPackage`	Maximum number of events in one package.	Default value: `1024`.

Setting	Description	Value
`UseRequestCountLimits`	Enable and disable regulating the number of events sent to the NDR server.	`Yes` (default value) – regulate the number of events sent. `No` – do not regulate the number of events.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	Default value: `3000`.
`EventLimitExceededPercentage`	Event throttle threshold (percentage). Sending events is limited if the ratio of events of a certain type to the total number of events exceeds the configured threshold (as a percentage).	Default value: `15`.
`PingPeriod`	NDR server polling period in seconds.	Default value: `450`.

How to verify that the KATA Integration is up and running

You can test Kaspersky Anti Targeted Attack Platform components in the following ways:

- On the command line using the following command:

  ```
  kesl-control --app-info
  ```

  For the integration with EDR (on-premises) and NDR (KATA) components, the **Available and running** status is displayed.

- In the Web Console:

  - In the Kaspersky Security Center console, using the *Report on status of application components*. For detailed information about reports, please refer to the Kaspersky Security Center Help.

  - In the OSMP Console:

    - Using the *Report on the status of application components*.

    - Go to the **Asset Management** → **Assets** section, select the **Analysis and response** tab.

      The device is displayed in the list with the **Normal activity** telemetry status.

    - Go to the **Threat hunting** section.

      Telemetry events from the device are displayed in the list of events.

- In Kaspersky Anti Targeted Attack Platform:

  Go to the **Assets** → **Devices** section. Devices are displayed in the table. If necessary, you can filter the table by **EPP application**, **EPP connection**, **Last connected to EPP**.

  Clicking the name of a device opens a pane. In the **Endpoint Agent** section, the connection status is **Active**.

Sandbox

The Sandbox technology makes it possible to analyze and scan objects on special servers with deployed virtual images of operating systems to detect malicious activity and indicators of targeted attacks on the corporate IT infrastructure.

The Kaspersky Endpoint Security application can interact with Sandbox via the Open Single Management Platform (OSMP) or the Kaspersky Anti Targeted Attack Platform.

> The component is not available for devices with an Elbrus CPU.

How to configure the Sandbox integration

Before you start configuring the Sandbox Integration:

- Allow inbound and outbound connections as follows:
  - Inbound (management interface):
    - TCP 22
    - TCP 443
    - TCP 8443
  - Outbound (management interface):
    - TCP 80 or TCP 443
  - Outbound and corresponding inbound directions (interface for access to processed objects):

    Any port.
- Install the graphical interface (the kesl-gui package) if you want to send files to the Sandbox manually from the context menu of a file or directory.

Essential configuration steps

1. **Create a Sandbox server connection request in the platform, then confirm the connection in the Sandbox management console**

   For details, refer to the Help for the respective solutions:

   - Kaspersky Anti Targeted Attack Platform
   - Open Single Management Platform

   Save the IP address of the Sandbox server in any convenient way. You will need it for subsequent configuration of the integration.

2. **Get and process the certificates issued by the OSMP server or the Central Node server**

   When integrating with Sandbox, devices running Kaspersky Endpoint Security establish encrypted HTTPS connections with the integration servers.

   > If the use of a proxy server is configured in the general settings of the Kaspersky Endpoint Security application, a proxy server is used for the connection to servers that handle the interaction with Sandbox.

Certificates for securing the connection with the servers that handle the interaction with Sandbox must be provided by the administrator of the OSMP platform or Kaspersky Anti Targeted Attack Platform.

To process certificates, follow the steps described in the Converting a PFX certificate to the PEM format article.

You can use a Server certificate and/or a Client certificate. The choice is determined by the security policy of your organization.

3 Manage Sandbox integration settings

To send files for scanning, you must enable the integration with KATA Sandbox and add a Central Node server that are deployed inside the solution.

How to configure the Sandbox integration in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Built-in Agents Configuration** → **Sandbox**.
5. In the **Type of file submission for scanning** drop-down list, select the required method:
   - **Manually**. In this mode, you can send objects for scanning to Sandbox manually using a command or from the **Scan in Sandbox** context menu.

     > We recommend selecting this type if your Sandbox version is older than 8.0.

   - **Automatically**. The application automatically sends objects for scanning, and it is impossible to manually send objects to be scanned by Sandbox.
   - **Combined**. The application automatically sends objects for scanning, but you can also send an object to Sandbox manually using a command or from the graphical interface.
6. In the **Connection to Sandbox servers** section:
   - Add the Integration Server by clicking the **Add** button in the toolbar.

     You can specify the IP address of the KATA / OSMP platform or its FQDN as the address.

     > If the Sandbox server is connected to OSMP, you can only specify the FQDN of the agent server.

   - Add the server certificate of Kaspersky Anti Targeted Attack Platform or OSMP that you received at step 2 of the main scenario.

     To do this, click the **Server connection settings** link, then in the displayed pane, in the **Server TLS certificate** section, click the **Upload** button.
   - If you need additional protection, create a crypto container.

To do this, in the **Additional connection security** section:

- Select the **Use two-way authentication** check box.
- Click the **Upload** button and add a client certificate.
- Enter a password for the crypto container in the corresponding field.

> The **Crypto-container password** field is mandatory. You cannot save the settings without entering a password for the client certificate (crypto container).

7. Select the relevant action in the **Action on threat detection** block:

- **Move copy to Quarantine, delete object**. If this option is selected, Kaspersky Endpoint Security deletes the malicious object found on the computer. Before deleting an object, Kaspersky Endpoint Security creates a backup copy of it in case you need to restore the object later. Kaspersky Endpoint Security moves the backup copy to Quarantine.
- **Run Critical Areas Scan**. If this option is selected, Kaspersky Endpoint Security runs the *Critical Areas Scan* task. By default, Kaspersky Endpoint Security scans the kernel memory, running processes, and boot sectors.
- **Create IOC Scan task**. If this option is selected, Kaspersky Endpoint Security automatically creates the *IOC Scan (autonomous IOC scan task)*. For this task, you can configure the run mode, scan scope, and action on IOC detection (*Move copy to Quarantine, delete object* or *Run Critical Areas Scan*). To modify other settings of the *IOC Scan* task, go to the task settings.

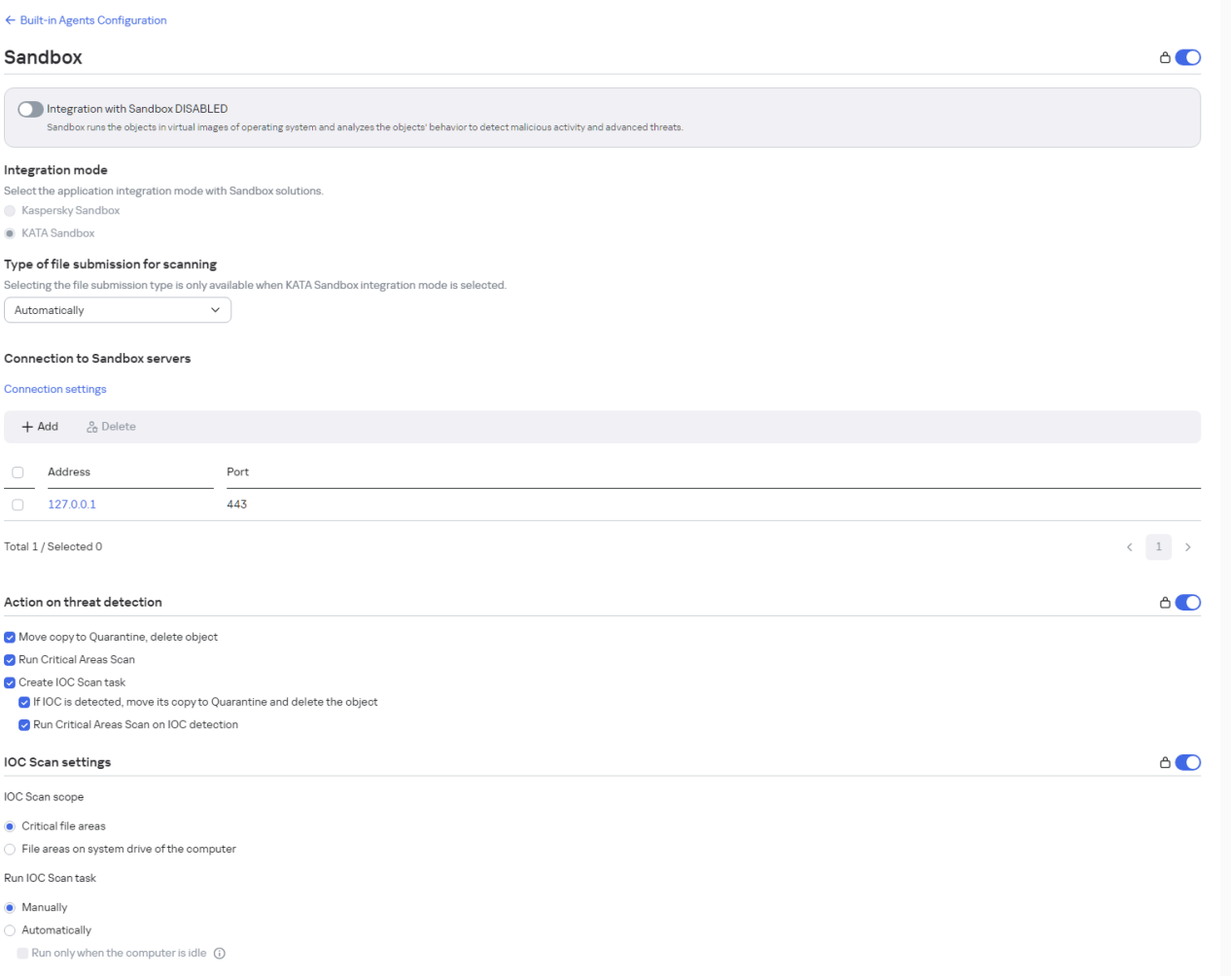
8. If necessary, configure the *IOC Scan* task settings in the **IOC Scan scope** block.

- **Critical file areas**. If this option is selected, Kaspersky Endpoint Security scans for IOCs only in user and system directories.
- **File areas on system drive of the computer**. If this option is selected, Kaspersky Endpoint Security scans all files in the root file system for IOCs.

9. If necessary, configure the *IOC Scan* task settings in the **Run IOC Scan task** block.

- **Manually**. Run mode in which you can start the *IOC Scan* task manually at a time when it is convenient for you.
- **Automatically**. Run mode in which Kaspersky Endpoint Security runs the *IOC Scan* task automatically after a threat is detected.

10. To apply the policy to computers, close the 🔒 padlock icons and save your changes.



Sandbox

How to configure the Sandbox integration on the command line

1. To add a server certificate, run the following command:

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

2. To add a Central Node or OSMP server, run the following command:

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port>
```

3. To configure integration settings, run the following command:

```
kesl-control --set-settings 29 [<setting name>=<setting value>]
```

The settings and their possible values are listed in the table below.

4. To add a client certificate, run the following command:

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

5. To enable Sandbox integration, run the following command:

```
kesl-control --start-task 29
```

Sandbox Integration task settings

Setting	Description	Value
`UseClientCertificate`	Enable and disable two-way authentication to further secure the connection to the Sandbox server. If client certificate validation is enabled on the Sandbox server side, enable the use of a client certificate and add a client certificate before starting the *Sandbox Integration* task.	`Yes` — use two-way authentication to further secure the connection to the Sandbox server. `No` (default value) — do not use two-way authentication.
`ConnectionTimeout`	Maximum time to wait for a connection to the server in seconds.	Default value: `10`.
`RequestTimeout`	Maximum time to wait for a response from the server in seconds.	Default value: `10`.
`SendingMode`	Mode of sending an object to Sandbox to be scanned	`AutoOnly` (default value) – automatically send files for scanning when an attempt is made to gain access to a file. `Manual` – send files for scanning manually. `AutoAndManual` – send files for scanning automatically as well as manually.
`QuarantineFile`	Quarantine file when a threat is detected.	`Yes` (default value) – if a threat is detected, delete the original file, place a copy of the file in Quarantine. `No` – do not quarantine the file when a threat is detected.
`ScanCriticalAreas`	Perform a critical areas scan when a threat is detected.	`Yes` (default value) – start a critical areas scan when a threat is detected. `No` – do not start a critical areas scan when a threat is detected.
`CreateIocScanTask`	Create an IOC Scan task when a threat is detected.	`Yes` (default) – create an IOC Scan task when a threat is detected. `No` – do not create an IOC Scan task when a threat is detected.
`QuarantineFileOnIocDetected`	Quarantine the object when an indicator of compromise is detected.	`Yes` (default value) – if an indicator of compromise is detected, delete the original object, place a copy of the object in Quarantine. `No` – do not quarantine the object when an indicator of compromise is detected.
`ScanCriticalAreasOnIocDetected`	Perform a critical areas scan when an indicator of compromise is detected.	`Yes` (default value) – start a critical areas scan when an indicator of compromise is detected. `No` – do not start a critical areas scan when an indicator of compromise is detected.
`Drives`	Scopes for the IoC scan.	`Critical` (default) – scan files in user and system directories. `System` – scan all files within the root file system.
`ScheduleMode`	IOC Scan task start mode.	`Manually` (default) – start the IOC Scan task manually. `AfterTreatDetected` – start the IOC Scan task after a threat is detected.
The **[Servers.item_#]** section contains the settings of the Sandbox server.		

Setting	Description	Value
`Address`	Address of the server. IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified.	Default value: `127.0.0.1`.
`Port`	Port for connecting to the server.	Default value: `443`.
The **[SandboxTransferSettings]** section contains settings for sending files for scanning in Sandbox.		
`SandboxQueue`	The maximum size of the scan request queue in megabytes.	Default value: `1024`.

4. **Verify that the connection to Sandbox has been established successfully**

   Check the status of Sandbox in any convenient way.

How to verify that the Sandbox Integration is up and running

You can test the Sandbox component in the following ways:

- On the command line using the following command:

  ```
  kesl-control --app-info
  ```

  Integration with Sandbox is displayed with the **Available and running** status.

- In the Web Console:

  - In the Kaspersky Security Center Console:

    Using the *Report on the status of application components*. For detailed information about reports, please refer to the Kaspersky Security Center Help.

  - In the OSMP Console:

    - Using the *Report on the status of application components*.

    - Go to the **Threat hunting** section.

      Successful Sandbox connection events are displayed in the list of events.

- In Kaspersky Anti Targeted Attack Platform:

  Go to the **Assets** → **Devices** section. Devices are displayed in the table. If necessary, you can filter the table by **EPP application**, **EPP connection**, **Last connected to EPP**.

  Clicking the name of a device opens a pane. In the Endpoint Agent section, the connection status is **Active**.

How to send a file to Sandbox manually

Kaspersky Endpoint Security allows users to manually send files or directories for scanning in Sandbox from the context menu.

To send files for scanning in Sandbox, the following conditions must be met:

- The graphical interface of Kaspersky Endpoint Security must be installed.
- Kaspersky Endpoint Security must be integrated with Sandbox.
- The mode of sending files for scanning must be set to **Manually** or **Combined**.

To send a file or directory for scanning in Sandbox:

1. Open the context menu of the file or directory that you want to scan.
2. Select **Kaspersky Endpoint Security 12.5 for Linux** as the application for opening the file or directory.

   Depending on the desktop environment, the names of the context menu commands may differ.

3. Then in the context menu, select **Scan in Sandbox**.

Kaspersky Managed Detection and Response

Kaspersky Endpoint Security includes a built-in agent for integration with the Kaspersky Managed Detection and Response solution. The *Kaspersky Managed Detection and Response (MDR)* solution automatically detects and analyzes security incidents in your infrastructure. To do so, MDR uses telemetry data received from endpoints and machine learning. MDR sends incident data to Kaspersky experts. The experts can then process the incident and, for example, add a new entry to Anti-Virus databases. Alternatively, the experts can issue recommendations on processing the incident and, for example, suggest isolating computer from the network. For detailed information about how the solution works, please refer to the Kaspersky Managed Detection and Response Help.

Integration is facilitated by a Kaspersky Endpoint Security component: Managed Detection and Response (MDR). The component must be activated in one of the ways described in the integration scenario.

The component is not available for devices with an Elbrus CPU.

Configurations of Kaspersky Endpoint Security for integrating with MDR

The following configurations can be used to work with MDR:

- **[KES+built-in agent]**. In this configuration, Kaspersky Endpoint Security acts as both the application that ensures the security of the computer and the application for working with MDR.
- **[third-party EPP+EDR Agent]**. In this configuration, the security of the IT infrastructure is provided by the third-party Endpoint Protection Platform (EPP). The interaction with MDR is provided by Kaspersky Endpoint Security in the Endpoint Detection and Response Agent (EDR Agent) configuration. In this configuration, EDR Agent is compatible with third-party EPP applications.

Recommendations for creating a reference image for correct integration with MDR

We do not recommend including the Kaspersky Endpoint Security for Linux application in the reference image.

If Kaspersky Endpoint Security for Linux was included in the reference image, follow these steps on each device based on this image:

1. To create a new UUID, run the following commands:

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
uuidgen > /var/opt/kaspersky/epagent/install_id
```

2. Uninstall Kaspersky Endpoint Security for Linux, then reinstall it.

If you do not follow these steps, the devices may not be identified correctly.

Uploading the KPSN configuration file

If your configuration does not satisfy the requirements for operation without KPSN configuration files, then to integrate with Kaspersky Managed Detection and Response, you need to upload a *KPSN configuration file* to the Kaspersky Security Center Administration Server. This file contains the necessary telemetry settings. The KPSN configuration file with the .pkcs7 extension is located in the ZIP archive of the MDR configuration file. For details, refer to Kaspersky Managed Detection and Response Help.

You can upload the KPSN configuration file in the Web Console or the Administration Console.

By uploading the KPSN configuration file, you agree that data from the device where Kaspersky Endpoint Security is installed will be automatically sent to Kaspersky for processing. Do not load the configuration file if you do not agree that the transmitted data will be processed. For detailed description of the transmitted data, refer to Kaspersky Managed Detection and Response documentation.

How to upload the KPSN configuration file in the Web Console

1. In the main Web Console window, open the Administration Server properties window.

2. In the list on the left, select the **KSN proxy server settings** section.

3. Turn on the **Enable KSN proxy server on the Administration Server as a proxy server** toggle switch to enable the KSN proxy server service.

4. Turn on the **Use Kaspersky Private Security Network** toggle switch.

5. In the window that opens and displays a warning about the specific aspects of using the KSN proxy server on the distribution points with the previous version of the Network Agent installed, click **OK**.

6. Click the **File with KSN proxy server settings** button.

7. Select the KSN configuration file (with the pkcs7 extension) and click **Open**.

8. Accept the terms and conditions of the KPSN Statement and click the **Save** button.

How to upload the KPSN configuration file in the Administration Console (MMC)

1. In the Administration Console tree, open the Administration Server properties window.

2. Select **KSN proxy server** → **KSN proxy server settings**.

3. Select the **Use Administration Server as a proxy server** check box to enable the KSN proxy server service.

4. Select the **Configure KPSN** check box.

5. In the window that opens and displays a warning about the specific aspects of using the KSN proxy server on the distribution points with the previous version of the Network Agent installed, click **OK**.

6. Click the **File with KSN proxy server settings** button.

7. Select the KSN configuration file (with the pkcs7 extension) and click **Open**.

8. Accept the terms and conditions of the KPSN Statement and click the **Apply** button.

How to upload the KPSN configuration file on the command line

Execute the command:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

How to configure the MDR integration

Before configuring the Kaspersky Managed Detection and Response integration:

- Allow connection on ports 443 and 1443.
- Allow connections to the following addresses:
  - *.ksn.kaspersky-labs.com
  - ksn-*.kaspersky-labs.com
  - ds.kaspersky.com

> The list of addresses is subject to change. To get the exact address, you can contact Technical Support.

- Make sure the following is enabled and working:
  - Kaspersky Security Network in extended mode:
  - Behavior Detection.

    To make sure the telemetry is complete, you can additionally enable the following components: Web Threat Protection, Network Threat Protection, File Threat Protection, and Mail Threat Protection.

Essential configuration steps

1. **Activate the MDR component in of the following ways**

   - Using a license key.

     Add the MDR license key to the application if you have purchased a separate license to use this functionality.

     If you are using Kaspersky Endpoint Security under a license that includes Kaspersky Managed Detection and Response, no action is required.

     > If Kaspersky Endpoint Security is used in Light Agent mode, the MDR license key is added to the SVM.

   - Using a MDR BLOB file.

     In the MDR Console, download the MDR configuration file. This file is a ZIP archive containing an MDR BLOB file and a KPSN configuration file.

     Then upload the BLOB file in the Web Console, the Administration Console, or on the command line.

   The version of the Kaspersky Endpoint Security application determines the method of activating the MDR component and whether you need to use the KPSN configuration file. For details, refer to Kaspersky Managed Detection and Response Help.

   > If the Kaspersky Security Center Administration Servers are organized in a hierarchy and the secondary server has no direct internet access, Kaspersky Managed Detection and Response cannot work even if the primary Administration Server has internet access.

2. **Upload the KPSN configuration file**

   If your organization has multiple tenants or you have activated the MDR component using an MDR BLOB, upload the KPSN file to the Kaspersky Security Center Administration Server. This file contains the necessary settings for sending telemetry; you can find it in the ZIP archive with the MDR configuration file.

3. **Configure the Kaspersky Managed Detection and Response integration settings**

   How to enable the Kaspersky Managed Detection and Response integration in the Web Console

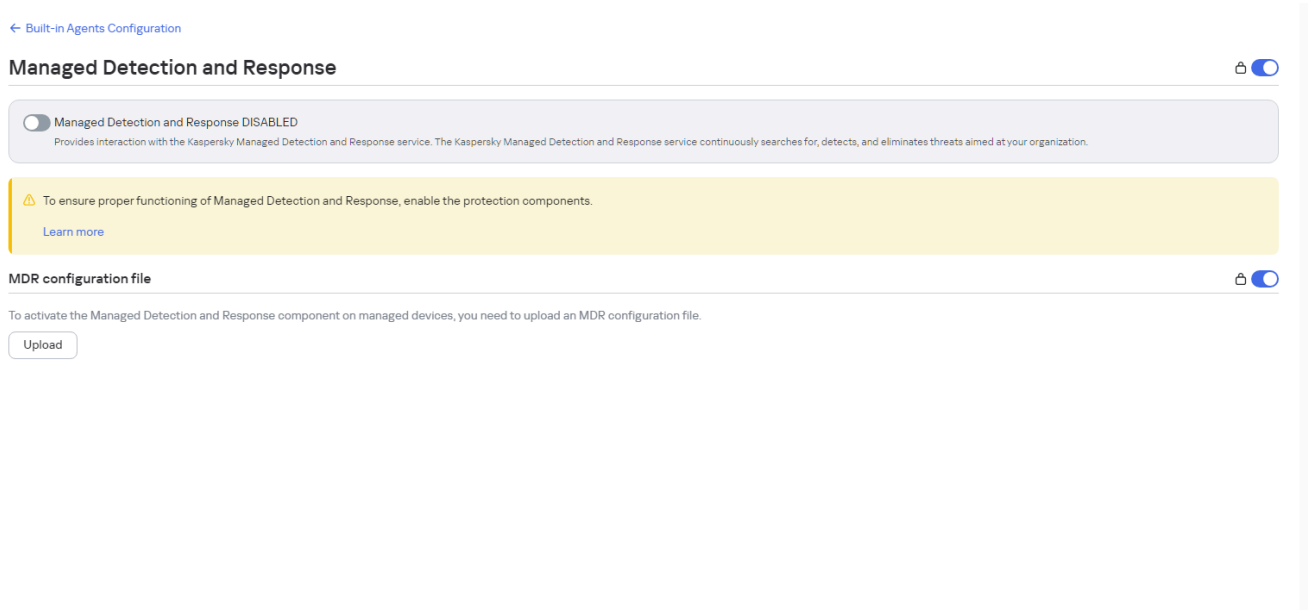
   1. In the main window of the Web Console, select the **Asset management** → **Policies** section.
   2. Click the required Kaspersky Endpoint Security policy.
   3. In the policy properties window that opens, select the **Application settings** tab.

4. In **Built-in Agents Configuration** section, select **Managed Detection and Response**, then in the right part of the screen, manage the following settings:

   - Set the toggle switch to **Managed Detection and Response ENABLED**.

   - If you have any tenants or if you have activated the MDR component using an MDR BLOB file, click the **Upload** button to add an MDR BLOB file.

5. Save the settings.



Managed Detection and Response

How to enable the Kaspersky Managed Detection and Response integration on the command line

1. To enable the MDR component, run the following command:

```
kesl-control --set-app-settings UseMDR=Yes
```

2. To add a BLOB file, run the following command:

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

4 Configure the KSN policy

How to manage KSN settings in the Web Console

1. In the Kaspersky Endpoint Security policy, on the **Application settings** tab, go to the **General Settings** section.

2. Select **Kaspersky Security Network**, then in the right part of the screen, specify the following settings:

   a. Set the toggle switch to **Use of Kaspersky Security Network (KSN) ENABLED**.

   b. In the **KSN Settings** subsection, select the **Use extended KSN mode** check box.

c. In the **KSN proxy server** subsection, select check boxes:

- **Use Administration Server as a KSN proxy server**
- **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**

Telemetry will be collected from the Administration Server or from the device, depending on whether the configured options are available.

3. Save the settings.

How to configure KSN settings on the command line

To enable KSN in extended mode, run the following command:

```
kesl-control --set-app-settings UseKSN=Extended --accept-ksn
```

5. **Enable KSN**

How to enable KSN in the Web Console

1. In the main menu, click the name of the Administration Server.
2. In the window that opens, on the **General** tab, select the **KSN Proxy** section.
3. Set the toggle switch to **Enable KSN Proxy on Administration Server Enabled**.
4. Enable a toggle switch depending on the KSN infrastructure solution that you are using:
   - **Use Kaspersky Security Network Enabled**.
   - **Use Kaspersky Private Security Network Enabled**, then upload the KPSN configuration file.
5. Save the settings.

6. **Make sure that the connection to Kaspersky Managed Detection and Response has been established successfully**

Check the status of Kaspersky Managed Detection and Response in any convenient way.

How to verify that the MDR Integration is enabled

You can check the health of the Kaspersky Managed Detection and Response component in the following ways:

- On the command line using the following command:

```
kesl-control --app-info
```

The Kaspersky Managed Detection and Response integration is displayed with the status **Available and running**.

- In the MDR Console, go to the **Assets** section. Devices are displayed with the **OK** (green) status.

If the component is disabled:

1. Update the application anti-virus databases.
2. Make sure that Kaspersky Security Network is enabled and running in extended mode.
3. Check the license keys for Kaspersky Endpoint Security and MDR.
4. Make sure the BLOB file has been added to the policy.
5. Verify that the components that MDR needs are in working order.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Linux supports the Kaspersky Unified Monitoring and Analysis Platform solution. *Kaspersky Unified Monitoring and Analysis Platform (KUMA)* is a security information and event management (SIEM) solution for the IT infrastructure of organizations. KUMA allows detecting, analyzing, and mitigating security threats before they can cause harm.

For more information about the solution, see the Kaspersky Unified Monitoring and Analysis Platform Help.

Kaspersky Endpoint Security is installed on individual computers on the corporate IT infrastructure and continuously monitors processes, open network connections, and files being modified. Information about events on the computer (telemetry) is sent to the Kaspersky Unified Monitoring and Analysis Platform (KUMA) server.

The component is not available for devices with an Elbrus CPU.

How to configure the KUMA integration

Before configuring the Kaspersky Unified Monitoring and Analysis Platform integration:

- Allow connection on ports 443 and 1443 or the ports configured on the KUMA collector side.
- Add the KUMA license key to the application if you have purchased a separate license to use this functionality.

  If you are using Kaspersky Endpoint Security under a license that includes Kaspersky Unified Monitoring and Analysis Platform, no action is required.

  If the application is used in Light Agent mode, the KUMA license key is added to the SVM.

Essential configuration steps

1. **In KUMA, configure a collector and a normalizer.**

   If you want to use a client certificate, when configuring the collector on the **Transport** tab, select the tcp connector type. Next, on the **Advanced settings** tab, in the **TLS mode** drop-down list, select **Custom PFX with client authentication**.

2. **Copy the address of the collector to connect to**

   In the **Resources** → **Active services** section in table of services, copy and save in any convenient way the values from the **FQDN / IP address** and **Port** columns.

   If you are using TLS for the connection, only specify the fully qualified domain name (FQDN). The setting value is case-sensitive.

3. **Get and process the certificates issued by the KUMA server**

   Using certificates for connection security is not supported for UDP connections to the KUMA server.

   A proxy server is used to connect to the KUMA server if use of a proxy server is configured in the general application settings of Kaspersky Endpoint Security.

   Get the Server certificate (Microservice CA Certificate), see Downloading CA certificates. To process the certificate, convert it to DER or PEM format by following the steps in the Converting a PFX certificate to the PEM format article.

   For added protection, you can also use a Client certificate obtained while configuring the collector, see step 1.

4. **Configure the Kaspersky Unified Monitoring and Analysis Platform integration settings**

   How to configure KUMA integration in the Kaspersky Security Center Web Console

   1. In the main window of the Web Console, select **Asset management** → **Policies**.
   2. Click the name of the Kaspersky Endpoint Security policy.

      The policy properties window opens.
   3. Select the **Application settings** tab.
   4. Go to **Built-in Agents Configuration** → **KUMA Integration**.
   5. Enable the **KUMA Integration ENABLED** toggle switch.
   6. Add KUMA servers:

      a. Click **Add**.

         This opens the form in which you can add KUMA servers.

      b. Select the protocol for connecting to the KUMA server: **HTTP/HTTPS**, **TCP**, **UDP**.

         The protocol for connecting to the collector in Kaspersky Endpoint Security must match the connector type in KUMA: **http**, **tcp**, or **udp**.

         If you select the **HTTP/HTTPS** protocol, by default, the application uses HTTPS for the connection to KUMA servers. To use HTTP, you need to manually specify this protocol in the server address (for example, `http://server.com`).

c. Enter the server address (IPv4, IPv6) and the port to connect to the server (by default, port 443 is specified).

You can view the server address in the connector properties in the KUMA console. For more information about KUMA connectors, see the Kaspersky Unified Monitoring and Analysis Platform Help.

d. Click **OK**.

Kaspersky Endpoint Security connects to the first KUMA server in the list. If the connection fails, Kaspersky Endpoint Security connects to the second KUMA server in the list and so on.

7. If necessary, configure the **Maximum delay when sending events (sec)** setting in the **Server connection settings** block. When the specified time runs out, Kaspersky Endpoint Security tries to connect to the same collector or connects to the next collector in the list if there are multiple collectors. The default setting is 30 seconds.

8. Save your changes.

How to configure the KUMA integration on the command line

1. To add a KUMA server, run the following command:

```
kesl-control --set-settings 33 Servers.item_001.ServerAddress=<kuma server address>
Servers.item_001.Port=<kuma server port> Servers.item_001.ServerProtocol=<tcp|HTTPWithCompression|udp>
```

2. To add a KUMA server certificate, run the following command:

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

3. To configure integration settings, run the following command:

```
kesl-control --set-settings 33 [<setting name>=<setting value>]
```

The settings and their possible values are listed in the table below.

4. To add a client certificate for the connection to the response server, run the following command:

```
kesl-control [-M] --add-kuma-client-certificate <path to the file>
```

5. To enable integration with EDR (KATA), run the following command:

```
kesl-control --start-task 33
```

Kaspersky Unified Monitoring and Analysis Platform Integration task settings

Setting	Description	Value
`UseTls`	Enable or disable the server certificate verification for additional protection of the connection to the KUMA server.	`Yes` — use a certificate to further secure the connection to the KUMA server. `No` (default) — do not use a certificate to secure the connection to the KUMA server.
`UseClientCertificate`	Enable and disable two-way authentication to further secure the connection to the KUMA server. If client certificate validation is enabled on the KUMA server side, enable the use of a client certificate and add a client certificate before starting the Kaspersky Unified Monitoring and Analysis Platform Integration task.	`Yes` – use two-way authentication to further secure the connection to the KUMA server. `No` (default value) — do not use two-way authentication.
`ConnectionTimeout`	Maximum time to wait for a connection to the KUMA server in seconds.	Default value: `5`.
The **[Servers.item_#]** section contains the settings of the KUMA server.		
`ServerAddress`	KUMA server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. If you set `UseTls=Yes`, you must specify the fully qualified domain name (FQDN) of the server from the certificate received when purchasing the license to use KUMA.	Default value: `127.0.0.1`.
`ServerPort`	Port to connect to the KUMA server.	Default value: `443`.
`ServerProtocol`	Protocol for connecting to the KUMA server.	`tcp` (default value) — use the TCP protocol to connect to the KUMA server. `HTTPWithCompression` — use the HTTP protocol with event compression to connect to the KUMA server. `udp` — use the UDP protocol to connect to the KUMA server. When the UDP protocol is selected, the use of certificates to provide connection protection is not supported (the values of the `UseTls`, `UseClientCertificate` and `ConnectionTimeout` settings are ignored), and there are no events about the connection to the KUMA server.
The **[KumaTransferSettings]** section contains settings for sending events to the KUMA server.		
`EventTransferTimeMax`	The maximum delay in sending events to the KUMA server in seconds.	Default value: `30`.

5. **Make sure that the connection to Kaspersky Unified Monitoring and Analysis Platform has been established successfully**

   Check the status of KUMA in any convenient way.

How to verify that the KUMA Integration is up and running

You can test the KUMA component in the following ways:

- On the command line using the following command:

  ```
  kesl-control --app-info
  ```

  Integration with KUMA is displayed with the **Available and running** status.

- In the Web Console (OSMP Console):

  Go to the **Threat Hunting** section: telemetry events with the "Connection to KUMA has been established" status for the relevant device are displayed in the event list.

- In Kaspersky Unified Monitoring and Analysis Platform:

  In the main menu of the KUMA console, go to the **Events** section: Kaspersky Endpoint Security telemetry events are displayed in the list.

Protection of virtual environments

Kaspersky Endpoint Security supports the Light Agent mode to work as part of Kaspersky Security for Virtualization Light Agent. *Kaspersky Security for Virtualization Light Agent* is an integrated solution that provides comprehensive protection of virtual machines against various types of information security threats, network attacks, and phishing attacks. To use this solution, you must install the application in Light Agent mode.

When you start Light Agent, it establishes and maintains a connection to the virtual machine SVM (Secure Virtual Machine). A Protection Server is deployed on the SVM. The *Protection Server* is the Kaspersky Security for Virtualization Light Agent solution component that scans files for viruses and other malware, updates anti-virus databases and manages license keys. Light Agent sends files or their fragments that need scanning to the SVM. Scan results are available for all virtual machines with Light Agent installed (the SharedCache technology). This technology increases the solution efficiency and provides a faster response to threats.

The infrastructure of the organization may contain many virtual machines with Light Agent installed and many SVMs. The Integration Server handles the interaction between virtual machines and SVMs. The *Integration Server* is a component of the Kaspersky Security for Virtualization Light Agent solution that generates a list of available SVMs and transfers this data to Light Agents, participates in the discovery of SVMs by Light Agents, protects the connection between Light Agents and SVMs, and performs other functions.

Connecting Light Agent to SVM

1. **Obtaining a list of available SVMs**

   Light Agent gets the list of available SVMs.

2. **Selecting the optimal Protection Server (SVM)**

   Light Agent determines an available Protection Server (SVM) that is optimal for connection according to the SVM selection algorithm.

3. **Checking additional connection settings**

   Light Agent checks additional SVM connection settings: tags, connection protection status, application functionality covered by the license.

4. **Connecting Light Agent to SVM**

   Light Agent establishes and maintains a connection with the selected SVM.

How to configure SVM discovery

You can select one of the SVM discovery methods for the Light Agent:

- Using the Integration Server (VIIS).

  Integration Server is the solution component that enables the interaction of Kaspersky Security for Virtualization Light Agent with the virtual infrastructure and generates a list of SVMs available for connection. Light Agent establishes a connection with the Integration Server and gets the list of SVM addresses.

  The Integration Server is most useful in large virtual infrastructures because it automatically balances the load between SVMs, gets information about available SVMs, analyzes this information, and provides Light Agents with a list of Protection Servers (SVMs) that are optimal for connection.

  For Light Agent to be able to get a list of SVMs, you only need to enter the address of the Integration Server.

- Using a high-availability cluster of Integration Servers.

  Deployment of a high-availability cluster of Integration Servers is available in Kaspersky Security for Virtualization Light Agent 6.4. A high-availability cluster of Integration Servers provides uninterrupted protection of the virtual environment thanks to the failover of SVMs and Light Agents to a backup Integration Server whenever the primary Integration Server fails. A special cluster component, the *load balancer*, is responsible for the server failover. For details about a high-availability cluster of Integration Servers, see the Kaspersky Security for Virtualization Light Agent Help.

  For the Light Agent to get a list of SVMs, you need to enter the address of the device on which the load balancer is installed.

- Using the list of SVM addresses.

  If you need to specify individual SVMs that you want Light Agent to connect to, you can prepare a list manually.

  You need to list addresses of available SVMs that the Light Agent can connect to.

How to configure SVM discovery by Light Agent in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.

2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to **Light Agent Mode** → **SVM discovery settings**.

5. Select an SVM discovery method.

   - **Use Integration Server**. Enter the settings for connecting to the Integration Server depending on your infrastructure:

     - **Single Integration Server**. Enter the Integration Server connection settings: IPv4 address or fully qualified domain name (FQDN) of the device.

     - **High-availability cluster of Integration Servers**. Enter the IP address and port of the load balancer that is part of the cluster.

   - **Use a custom list of SVM addresses**. Create a list of SVMs that Light Agent can connect to. Specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of SVM. Each list item must be entered on a new line or separated from the previous item with a semicolon (`;`) character.

     > In the list of SVM addresses, specify only full domain names (FQDN) that are matched by a single IP address. Using a fully qualified domain name that corresponds to multiple IP addresses can lead to errors in the solution.

6. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

To view information about connecting Light Agent to the Integration Server on the command line:

1. Make sure the application is installed in Light Agent mode:

   ```
   kesl-control -V --ksvla-info
   ```

   The component must have the **On** status.

2. Output information about the Light Agent's connection to the Integration Server:

   ```
   kesl-control -V --viis-info
   ```

The command outputs the following information to the console:

- Address and port of the Integration Server that the Light Agent connects to.
- Status of the connection to the Integration Server.
- Date and time of the last connection between the Light Agent and the Integration Server.

How to view the information about the Light Agent's connection to the Integration Server on the command line

1. Make sure the application is installed in Light Agent mode:

   ```
   kesl-control -V --ksvla-info
   ```

   The component must have the **On** status.

2. Output information about the Light Agent's connection to the Integration Server:

```
kesl-control -V --svm-info
```

The command outputs the following information to the console:

- The address of the SVM to which the Light Agent is connected, and the location of the SVM in the virtual infrastructure relative to the Light Agent: local or not local.
- SVM discovery method that the Light Agent uses: using an Integration Server or using a custom list of SVM addresses.
- List of SVM addresses, if the selected SVM discovery method is lists of SVM addresses.
- Tag for connecting Light Agent to the SVM.
- SVM selection algorithm: standard or advanced. If the extended SVM selection algorithm is used, the type of the SVM's location in the virtual infrastructure is also displayed.
- Protection of the connection between the Light Agent and the Protection Server.

How Light Agent selects SVMs

The infrastructure of the organization may have multiple deployed SVMs to which Light Agents can connect. To balance the load on the network and resources of the virtual infrastructure, you need to distribute the Light Agents among the SVMs.

SVM selection algorithms

Light Agents can apply the following SVM selection algorithms for connection: Standard algorithm (by default) and Extended algorithm.

Standard algorithm	Extended algorithm
If this algorithm is used, after installation and startup, the Light Agent on the virtual machine chooses to connect to an SVM that is *local* with respect to the Light Agent. If no local SVMs suitable for connection are to be found, the Light Agent selects an SVM to which the least number of Light Agents is connected, regardless of the position of the SVM in the virtual infrastructure. The application does not determine whether the SVM is local relative to the Light Agent if large infrastructure protection mode is enabled for the Protection Server on the SVM. In this case, it is recommended to use the extended SVM selection algorithm and select the Integration Server as the SVM discovery method. Whether an SVM is considered local to a Light Agent depends on the type of virtual infrastructure.	If this algorithm is applied, you can define the following SVM selection settings: • whether to consider or ignore the SVM location in the infrastructure when choosing SVMs for connection • if the SVM location is considered, the method for determining SVM locality relative to the Light Agent If Light Agents ignore the location of SVMs in the infrastructure, Light Agents will be able to connect to any SVMs available for connection. If Light Agents must consider the location of SVMs in the infrastructure, you need to select the SVM path type that will be considered when determining the SVM locality relative to the Light Agent. Whether an SVM is considered local to the Light Agent depends on the type of virtual infrastructure. If Light Agents consider the location of SVMs in the infrastructure when choosing which SVM to connect to, Light Agents can only connect to SVMs that are local. For example, if you specify a hypervisor cluster as the SVM path type, all SVMs deployed on this hypervisor cluster will be considered local to the Light Agent, and the Light Agent can connect only to one of these SVMs. If there are no SVMs available for connection in the same cluster in which the Light Agent is running, the Light Agent does not connect to an SVM. When selecting SVMs, Light Agents also consider the number of connected Light Agents to ensure that Light Agents are evenly distributed among SVMs available for connection. If the Light Agent uses the extended SVM selection algorithm and the SVM discovery method is set to SVM address list, and large infrastructure protection mode is enabled on the SVM, then connecting a Light Agent to this SVM is only possible if the SVM path is ignored.
Basis Dynamix Enterprise	
In a virtual infrastructure based on Basis Dynamix Enterprise, the SVM that is considered to be local to a Light Agent is the SVM that is deployed on the same node as the virtual machine with the Light Agent installed.	In a virtual infrastructure based on Basis Dynamix Enterprise, an SVM can be considered local to the Light Agent in any one of the following cases: • An SVM is deployed on the same node as the virtual machine with the Light Agent installed. • An SVM is deployed in the same zone as the virtual machine with the Light Agent installed. • An SVM is deployed in the same data center as the virtual machine with the Light Agent installed.
Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, and Basis Dynamix Standard	
In a virtual infrastructure based on Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer or Basis Dynamix Standard, the SVM that is considered to be local to a Light Agent is the SVM that is deployed on the same hypervisor as the virtual machine with the Light Agent installed.	In a virtual infrastructure based on Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer or Basis Dynamix Standard, an SVM can be considered local to the Light Agent in any one of the following cases: • An SVM is deployed on the same hypervisor as the virtual machine with the Light Agent installed. • An SVM is deployed on the same hypervisor cluster as the virtual machine with the Light Agent installed. • An SVM is deployed in the same data center as the virtual machine with the Light Agent installed.
OpenStack and VK Private Cloud SVM	

Standard algorithm	Extended algorithm
In a virtual infrastructure running on the OpenStack or VK Private Cloud platform, you can specify how to determine SVM locality relative to the Light Agent using the `StandardAlgorithmSvmLocality` parameter in the `HypervisorSpecificSettings:Openstack` section of the Integration Server configuration file appsettings.json. Depending on the version of the Integration Server, the file is located at one of the following paths: • /var/opt/kaspersky/viis/common/ for the Linux-based Integration Server • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ for the Windows-based Integration Server The `StandardAlgorithmSvmLocality` parameter can take the following values: • `ServerGroup` – if this value is selected, SVM is considered local to the Light Agent if it is located within the same server group as the virtual machine with the Light Agent installed. This value is used by default. • `Project` – if this value is selected, SVM is considered local to the Light Agent if it is deployed within the same OpenStack project as the virtual machine with the Light Agent installed. • `AvailabilityZone` – if this value is selected, SVM is considered local to the Light Agent if it is located within the same availability zone as the virtual machine with the Light Agent installed.	In a virtual infrastructure running on the OpenStack or VK Private Cloud platform, an SVM can be considered local to the Light Agent in any one of the following cases: • An SVM is located in the same server group as the virtual machine with the Light Agent installed. • An SVM is deployed within the same OpenStack project as the virtual machine with the Light Agent installed. • An SVM is located in the same availability zone as the virtual machine with the Light Agent installed.

In addition to SVM connection algorithms, you can regulate the connection of Light Agents to SVMs using tags.

How to configure the SVM selection algorithm for Light Agent in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Light Agent Mode** → **SVM selection algorithm**.
5. Select the algorithm:
   - **Use the standard SVM selection algorithm**. Light Agent selects SVMs, deployed in the same hypervisor.
   - **Use the extended SVM selection algorithm**. Light Agent selects SVMs deployed in the selected SVM path type (by default, **Hypervisor**).
6. If necessary select SVM path for the extended SVM selection algorithm:
   - **Hypervisor**. The Light Agent selects an SVM to connect to that meets the criteria (depending on the type of virtual infrastructure):
     - The SVM are deployed on the same hypervisor as the virtual machine with the Light Agent installed (in a virtual infrastructure based on Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, or Basis Dynamix Standard).
     - The SVM is located in the same server group as the virtual machine with the Light Agent installed (in a virtual infrastructure running on the OpenStack or VK Private Cloud platform).
     - The SVM is located on the same node as the virtual machine with the Light Agent installed (in a virtual infrastructure Basis Dynamix Enterprise).

     If there are no SVMs available for connection on the same hypervisor or in the same Server Group where the virtual machine with the Light Agent is located, the Light Agent does not connect to the SVM.

- **Cluster**. The Light Agent selects an SVM to connect to that meets the criteria (depending on the type of virtual infrastructure):

  - The SVMs are deployed in the same hypervisor cluster as the virtual machine with the Light Agent installed (in a virtual infrastructure based on Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, or Basis Dynamix Standard).

  - The SVMs are deployed within the same OpenStack project as the virtual machine with the Light Agent installed (in a virtual infrastructure running on the OpenStack or VK Private Cloud platform).

  - The SVM is located in the same zone as the virtual machine with the Light Agent installed (in a virtual infrastructure Basis Dynamix Enterprise).

  If there are no SVMs available for connection in the same hypervisor cluster or within the same OpenStack project where the virtual machine with the Light Agent is located, the Light Agent does not connect to the SVM.

- **Data center**. The Light Agent selects an SVM to connect to that meets the criteria (depending on the type of virtual infrastructure):

  - The SVMs are deployed in the same data center as the virtual machine with the Light Agent installed (in a virtual infrastructure based on Microsoft Hyper-V, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, or Basis Dynamix Standard).

  - The SVMs are located in the same Availability Zone as the virtual machine with the Light Agent installed (in a virtual infrastructure running on the OpenStack or VK Private Cloud platform).

  - The SVM is located in the same data center as the virtual machine with the Light Agent installed (in a virtual infrastructure Basis Dynamix Enterprise).

  If there are no SVMs available for connection in the same data center or Availability Zone where the virtual machine with the Light Agent is located, the Light Agent does not connect to the SVM.

- **Ignore**. Light Agent ignores the SVM path for connecting to the Protection Server. Light Agents takes into account other criteria: tags, the number of Light Agents connected to an SVM, and so on.

7. To apply the policy to computers, close the 🔒 padlock icons and save your changes.

How to balance the connection of Light Agents among SVMs

Multiple Light Agents can connect to an SVM. To balance the Light Agent connections, you can specify a separate list of SVMs. If you are using an Integration server for SVM discovery, you can use *tags* to balance Light Agent connections to SVMs. That is, for a Light Agent, you can assign a list of SVMs for connecting using a tag. To do so, you must assign a tag to the Light Agent and specify this tag in SVM settings. For details about specifying tags in SVM settings, see the Kaspersky Security for Virtualization Light Agent Help.

Example: The Kaspersky Endpoint Detection and Response Optimum solution is deployed in your infrastructure for designated virtual machine hosts. In this case, you can assign the `[EDROptimum]` tag to the Light Agent to make it connect to the SVMs that has the EDR Optimum (EDR Optimum Add-on) license key added. As a result, you can use EDR Optimum functionality on the virtual machine with the Light Agent. When connecting the Light Agent to an SVM without an EDR Optimum license key, Kaspersky Endpoint Detection and Response Optimum functionality is unavailable.

How to assign an SVM connection tag to a Light Agent in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Light Agent Mode** → **SVM connection tag**.
5. Select the **Use connection tag** check box and enter SVM connection tag.

   For a tag, you can enter a text string up to 255 characters long. You can use any character except the `;` character.
6. To apply the policy to computers, close the padlock icons and save your changes.

Protecting the connection between Light Agent and an SVM

You can configure encryption of the connection between Light Agents and Protection Server. To do this, you need to enable the encryption of the data channel between Light Agent and the Protection Server in the Protection Server settings on the SVM and in the Light Agent settings.

A Light Agent for which connection protection is enabled can only connect to SVMs for which encryption of the data channel between the Light Agent and the Protection Server is enabled. A Light Agent for which connection protection is disabled can only connect to SVMs for which channel encryption is disabled or an insecure connection between the Protection Server and the Light Agent is allowed.

For details about configuring connection protection on the Protection Server, see the Kaspersky Security for Virtualization Light Agent Help.

Protecting the connection using encryption may reduce the performance of Kaspersky Security for Virtualization Light Agent.

How to configure connection protection in a Light Agent in Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to **Light Agent Mode** → **Connection protection**.
5. Select the **Encrypt data channel between Light Agent and the Protection Server** check box.
6. To apply the policy to computers, close the padlock icons and save your changes.

How to find out the status of the Light Agent

On the command line, you can view the following information about the application being used in Light Agent mode:

- Settings for using the application in Light Agent mode
- Connecting the Light Agent to the Integration Server
- Connecting the Light Agent to SVMs

Viewing information about settings for using the application in Light Agent mode

```
kesl-control [-V] --ksvla-info
```

The command outputs the following information to the console:

- Light Agent mode for protecting virtual environments: On or Off.

  If Light Agent mode is enabled, the application is used as part of the Kaspersky Security for Virtualization Light Agent solution.

- VDI protection mode: On or Off.

  VDI protection mode optimizes the Kaspersky Endpoint Security for running on temporary virtual machines. If VDI protection mode is enabled, updates that require restarting the protected virtual machine are not installed on temporary virtual machines. When receiving updates that require a restart, the Light Agent installed on a temporary virtual machine sends a message to Kaspersky Security Center about the need to update the protected virtual machine template.

- Virtual machine type: persistent or nonpersistent.
- Virtual machine role: Server or Workstation.
- Virtual machine ID – UUID.

Viewing information about the Light Agent's connection to the Integration Server

```
kesl-control [-V] --viis-info
```

The command outputs the following information to the console:

- Address and port of the Integration Server that the Light Agent connects to.
- Status of the connection to the Integration Server.
- Date and time of the last connection between the Light Agent and the Integration Server.

If your infrastructure has a Linux-based high-availability cluster, the address and port of the load balancer are displayed. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

Viewing information about the Light Agent's connection to an SVM

```
kesl-control [-V] --svm-info
```

The command outputs the following information to the console:

- The address of the SVM to which the Light Agent is connected, and the location of the SVM in the virtual infrastructure relative to the Light Agent: local or not local.
- SVM discovery method that the Light Agent uses: using an Integration Server or using a custom list of SVM addresses.
- List of SVM addresses, if the selected SVM discovery method is lists of SVM addresses.
- Tag for connecting Light Agent to the SVM.
- SVM selection algorithm: standard or advanced. If the extended SVM selection algorithm is used, the type of the SVM's location in the virtual infrastructure is also displayed.
- Protection of the connection between the Light Agent and the Protection Server.

For information about the settings for connecting Light Agents to the Integration Server and SVMs, refer to the Kaspersky Security for Virtualization Light Agent Help.

Best practices

When deploying Kaspersky Endpoint Security for Linux, you can use the recommendations described in this section to configure computer protection and optimize performance. For more information on dealing with computer performance issues, please refer to the Technical Support Knowledge Base.

Optimizing resource consumption by the application

The application running with default settings may impact system performance on some devices because of the same resources being used by your applications and Kaspersky Endpoint Security.

Recommended configuration scenario to optimize system resource consumption by the application:

1. **Put your devices in administration groups according to the role of each device in the infrastructure.**

   Take an inventory of devices and the functions they perform and put them in different administration groups based on those functions. For example, you can have an administration group with web servers, another administration group with database servers, a third administration group with user workstations, and so on.

2. **Configure the application for typical server roles.**

   Configure the application on devices according to their role in the infrastructure as recommended.

3. **Analyze the performance on pilot devices.**

   Pick one or two pilot devices in each administration group. For each device, analyze how Kaspersky Endpoint Security uses system resources and how this impacts the performance of installed applications.

4. **Configure the application on pilot devices based on the results of performance analysis.**

   If the performance of applications is significantly degraded or the amount of system resources consumed by Kaspersky Endpoint Security is critical for the operation of the operating system and applications, configure File Threat Protection and scan tasks as recommended.

   To reduce the impact of the Web Threat Protection, Network Threat Protection, and Behavior Detection components on the performance of your applications, optimize the performance of these components.

5. **Configuring the application on all devices.**

   If the above steps helped improve performance on your pilot device, make the same changes on other devices of the same type.

Analysis of application performance on the device

When scanning objects, Kaspersky Endpoint Security uses CPU resources, disk subsystem input/output, and RAM.

View information about resource consumption by the application

```
top -bn1|grep kesl
```

The command must be executed when the system is under load.

The command output shows the amount of used memory and processor time:

```
651 root        20      0 3014172 2.302g 154360 S 120.0 30.0    0:32.80 kesl
```

Column 6 displays the amount of resident memory: 2.302g.

Column 9 displays the percentage of the processor cores usage – 120.0, where each core is represented by 100 percent. Thus, 120% means that one core is fully used, and the other is used at 20%.

To get information about the performance of the application, you can also configure the collection of metrics for operating system resources that the application uses.

If Kaspersky Endpoint Security critically slows down your system, you need to find out which application components and tasks are taking up system resources.

To do this, perform the following experiments on the device:

1. **Analyze the resource consumption of the File Threat Protection task (task of the OAS type)**

   In this way, you can find out if the performance issues are related to the File Threat Protection task or the scan tasks (tasks of the ODS and ContainerScan types), and follow the recommendations for the relevant tasks.

   How to analyze the resource consumption of the File Threat Protection task

   1. Stop all scan and monitoring tasks.

   2. Make sure that on-demand scan tasks (tasks of the ODS and ContainerScan types) are not scheduled to run during your investigation:

      a. Get a list of all application tasks:

      ```
      kesl-control --get-task-list
      ```

      b. Get the schedule settings for all tasks of the ODS and ContainerScan types:

      ```
      kesl-control --get-schedule <task ID |name>
      ```

      If the command output is `RuleType=Manual`, the task can only be started manually.

c. For all tasks that have a `RuleType` other than `Manual`, change the schedule:

```
kesl-control --set-schedule <task ID |name> RuleType=Manual
```

3. Enable generation of application trace files with a high level of details:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. If the File Threat Protection task is not running, start it:

```
kesl-control --start-task 1
```

5. Apply load to the system in the same mode that caused the performance problems. A few hours is enough.

6. Analyze the resulting trace files. By default, trace files are saved in the /var/log/kaspersky/kesl/ directory.

   Under load, the application writes a lot of information to the trace files; however only 10 files 500 MB each are kept, meaning that older information is overwritten.

   If performance and resource consumption issues persist, you may need to optimize File Threat Protection.

   If performance and resource consumption issues no longer occur, then the most likely cause of the issues are the on-demand scan tasks (tasks of the ODS and ContainerScan types) or the Behavior Detection task. You need to optimize scan tasks or analyze the performance of the Behavior Detection task.

7. Disable application trace file creation:

```
kesl-control --set-app-settings TraceLevel=None
```

2 Analyze resource usage by the Behavior Detection task (task of the Behavior_Detection type).

In this way, you can find out if the performance issues are related to the Behavior Detection task or the scan tasks (tasks of the ODS and ContainerScan types), and follow the recommendations for the relevant tasks.

How to analyze resource usage by the Behavior Detection task

1. Stop all scan and monitoring tasks.

2. Make sure that on-demand scan tasks (tasks of the ODS and ContainerScan types) are not scheduled to run during your investigation:

   a. Get a list of all application tasks:

```
kesl-control --get-task-list
```

b. Get the schedule settings for all tasks of the ODS and ContainerScan types:

```
kesl-control --get-schedule <task ID|name>
```

If the command output is `RuleType=Manual`, the task can only be started manually.

c. For all tasks that have a `RuleType` other than `Manual`, change the schedule:

```
kesl-control --set-schedule <task ID|name> RuleType=Manual
```

3. Enable generation of application trace files with a high level of details:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Run the Behavior Detection task if it is not running:

```
kesl-control --start-task 20
```

5. Apply load to the system in the same mode that caused the performance problems. A few hours is enough.

6. Analyze the resulting trace files. By default, trace files are saved in the /var/log/kaspersky/kesl/ directory.

> Under load, the application writes a lot of information to the trace files; however only 10 files 500 MB each are kept, meaning that older information is overwritten.

If performance and resource consumption issues persist, you may need to optimize Behavior Detection.

If performance and resource consumption issues no longer occur, then the most likely cause of the issues are the on-demand scan tasks (tasks of the ODS and ContainerScan types). This means you need to optimize these tasks.

7. Disable application trace file creation:

```
kesl-control --set-app-settings TraceLevel=None
```

3 Identify the most frequently scanned objects

You can exclude non-dangerous frequently scanned objects and files from scanning to optimize the performance of File Threat Protection and scan tasks.

Determine whether the objects scanned the most number of times are dangerous. For example, database files, directories, and log files can be considered safe if a write operation is performed by a trusted process. In case of any difficulties, contact Technical Support.

How to identify the most frequently scanned objects

1. Get the list of objects that have been scanned the most times:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -
r|less
```

The result is loaded into the less text viewer utility, where the objects that have been scanned the most times are displayed first.

If you need to aggregate object scanning statistics in subdirectories down to a certain depth starting from the root directory `/`, you can add `cut -d/ -f 1-X` to the command, where X is the nesting depth. For example:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | cut -d/ -f 1-4 | sort | uniq -c |
sort -k1 -n -r|less
```

2. If various services frequently write data to files in the system, such files are scanned again in the pending queue. Get the list of paths that have been scanned the most times in the pending queue:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
sort | uniq -c | sort -k1 -n -r
```

The files that were scanned the most times will appear at the beginning of the list.

If you need to aggregate object scanning statistics in subdirectories down to a certain depth starting from the root directory `/`, you can add `cut -d/ -f 1-X` to the command, where X is the nesting depth. For example:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $10}' |
tr -d ',' |  cut -d/ -f 1-3 | sort | uniq -c | sort -k1 -n -r
```

4. **Identify processes for which Kaspersky Endpoint Security detects starting most often**

You can exclude non-dangerous, frequently started processes from scanning to optimize the performance of Behavior Detection.

How to identify the most frequently started processes

Execute the command:

```
kesl-control --get-statistic --processes
```

This command outputs the list of processes whose starts Kaspersky Endpoint Security detects most frequently, and the start count for these projects.

5. **Identify paths at which the most file operation interceptions occur**

You can exclude directories from file operation interception to optimize the performance of File Threat Protection and scan tasks.

How to get information about file operation interception

You can get information about file operation interception in the following ways:

- Get statistics for files that the File Threat Protection component scans most often:

  ```
  kesl-control --get-statistic --files
  ```

  This command lets you display file operation interception statistics over the last 24 hours.

- Use application trace files for more detailed analysis. By analyzing trace files, you can get a list of files intercepted by the application and identify paths associated with a lot of file operation interception.

  By default, the application does not generate trace files.

  ```
  Enable trace file creation
  kesl-control --set-app-settings TraceLevel=Detailed
  ```

  Enabling tracing may impact overall system performance. We recommend disabling tracing when you no longer need trace files.

  ```
  Disable trace file creation
  kesl-control --set-app-settings TraceLevel=None
  ```

- Get a list of intercepted files:

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'|sort | uniq -c | sort -k1 -n -r
  ```

  If you need to aggregate file operation interception statistics in subdirectories down to a certain depth starting from the root directory `/`, you can add `cut -d/ -f 1-X` to the command, where X is the nesting depth. For example:

  ```
  grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | tr -d '}'|awk -F':' '{print $2}'| cut -d/ -f 1-3|sort | uniq -c | sort -k1 -n -r|less
  ```

You can analyze the performance of the application on the command line. If the device is managed by a Kaspersky Security Center policy, allow local task management while you carry out your investigation.

Recommendations for File Threat Protection and scan tasks

General recommendations

Scan exclusions

Scan exclusions help balance system security with performance.

We recommend excluding the following from scanning:

- Data files and index files of databases. According to virus experts at Kaspersky, there is no danger of viruses spreading through such files.
- Safe objects from the list of most frequently scanned objects.

You can configure exclusions by file path (you can also specify the mount type), file mask, threat type, and path to the process performing file operations.

> The application does not scan objects excluded from scanning, but file operations still experience minimal delays because the application still performs file operation interception and blocking. If you need to prevent even minimal delays, we recommend configuring exclusions from file operation interception.

How to configure exclusions:

- You can configure File Threat Protection exclusions in a policy using the Web Console or Administration Console, or locally on the device using the command line.
- You can configure exclusions for scan tasks of the ODS and ContainerScan types in the task settings in Kaspersky Security Center or locally on the device using the command line.

  > Exclusions configured for one scan task do not affect other scan tasks. Exclusions must be configured separately for each scan task.

Examples of File Threat Protection exclusions configured on the command line

```
Exclude the /tmp/logs directory and all subdirectories and files recursively
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

```
Exclude a specific file or files by mask in the /tmp/logs directory
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

```
Exclude all files with the .log extension in the /tmp directory and subdirectories using a recursive mask
```

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Exclusions from file operation interception

Files excluded from scanning may still be intercepted by the application during File Threat Protection and scanning tasks. The application intercepts file operation events and blocks actions until the events are processed. After the scan, the application can:

- Unblock and allow the operation.
- Block the operation and perform the actions specified in protection or verification settings.

Intercepting events takes time, which affects the performance of other applications and the operating system.

> If your operating system supports the fanotify technology and satisfies requirements, configure the updatable kernel module for the application. The updatable kernel module is included in the distribution kit of the application. The updatable kernel module allows optimizing file operation interception.

To exclude files in a certain directory not only from scanning, but also from interception, configure exclusion for mount points (global exclusions). Exclusion of mount points allows you to exclude local or remote directories mounted on a device from interception of file operations.

You can view the list of mount points detected on the device using the Web Console, Administration Console, or the command line. The list displays information indicating whether the mount point has been added to scan exclusions.

Kaspersky experts recommend using global exclusions in the following cases:

- The connection to a mounted remote resource, such as NFS or SMB, is slow.
- Even minimal lag is not acceptable.

You can specify the mount point type (Local, AllRemoteMounted, Mounted:NFS, Mounted:SMB, or Mounted:Custom) or specific mount points. The application does not monitor excluded scopes.

> To protect shared network resources, use the Kaspersky Endpoint Security application on the device where the resources are physically stored.

If you use the updatable kernel module for system event interception, you can exclude from interception individual local or remote directories mounted on the device, not just the entire mount points.

> If you use fanotify for system event interception, global exclusions do not apply to paths that are not mount points.

You can configure global exclusions in a policy using the Web Console or Administration Console, or locally on the device using the command line.

Example of a global exclusion configured for the /tmp directory using the command line

To exclude all files in the /tmp directory from interception:

1. If you use fanotify for system event interception, check if the /tmp directory is a mount point:

   ```
   mount
   ```

If the directory is absent from the output of the mount command:

a. Create a mount point:

```
mount --bind /tmp/ /tmp
```

b. Add the following line to the /etc/fstab file to make the newly created mount point persist in the system after restart:

```
/tmp /tmp none defaults,bind 0 0
```

If you are using the updatable kernel module for system event interception, skip this step.

2. Add the /tmp directory to global exclusions:

```
kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
```

3. Restart the application to apply global exclusions:

```
systemctl restart kesl
```

Limiting RAM usage by the application

You can limit the amount of RAM that Kaspersky Endpoint Security uses when scanning files with the File Threat Protection component and when performing scan tasks of the ODS and ContainerScan types.

Limiting memory usage can be useful for systems with a large amount of RAM (more than 5 GB).

By default, the application may use up to 8192 MB of RAM. You can adjust the amount of RAM used by the application:

- In the policy, using the **Memory usage limit for scan tasks (MB)** setting.
- Locally on the device using the `ScanMemoryLimit` setting in the kesl.ini configuration file.

If the specified value is less than 2 MB, the application uses the minimum value (2 MB). If the specified value is greater than the amount of RAM available on the device, the application uses up to 25% of the RAM. This value cannot be changed.

> This setting limits only the amount of memory used when scanning files. That means that the total amount of memory required by the application can be more than the value of this setting.

Additional recommendations for File Threat Protection

Scan only when opening a file

Change the file scanning mode to scan a file only when the file is opened. By default, the application scans a file when something attempts to open it, and scan it again when something attempts to close it, if the file was modified.

You can change the file scanning mode in the File Threat Protection settings:

- In the policy using the Web Console or Administration Console: set **File Threat Protection mode** to **When opened**.
- Locally on the device:

```
kesl-control --set-set 1 ScanByAccessType=Open
```

Changes made to the file after it is opened are not scanned until the next opening of the file.

Scanning archives

Make sure that archive scanning is disabled (default setting). Scanning archives impacts performance because access to the archive file is blocked while the file is being unpacked to the /tmp temporary directory and scanned. The definition of archive includes traditional archives as well as packaged objects such as .jar.

You can enable or disable archive scanning using the Web Console or Administration Console (the **Scan archives** setting) or locally on the device using the command line (the `ScanArchived` setting).

Scanning files copied from network directories

Configure a scan exclusion for files copied from network directories. Files are scanned only after the process of copying to a local directory is finished.

To exclude files located in network directories from scans, configure exclusion based on processes for the utility used for copying from network directories (for example, for the `cp` utility).

If you manage the application using Kaspersky Security Center, you can configure exclusion based on processes in the Web Console or the Administration Console. If you are administering the application using the command line, you can configure an exclusion by process by adding an `[ExcludedForProgram.item_#]` section to the settings of the OAS task.

Additional recommendations for scan tasks

Task launch schedule

Schedule scan tasks so that they do not overlap. The application allows running scan tasks simultaneously, but this may significantly increase resource consumption. Check the schedule of all ODS and ContainerScan tasks locally on the device or in Kaspersky Security Center.

Run the scan during the minimum server load.

Scanning remote directories

Make sure that the scope of the scan tasks does not include any remote directories mounted on the device via SMB or NFS.

We recommend scanning such directories directly on the device that provides the resource. If this is not possible, do not perform the scan on servers that run critical services, because such a task may take quite a long time (depending on the connection speed and the number of files).

Using global exclusions and File Threat Protection exclusions

Make sure that the following settings are enabled for the Malware scan task:

- **Use global exclusions** (`UseGlobalExclusions`) to exclude mount points specified in global exclusions from scanning.
- **Use File Threat Protection exclusions** (`UseOASExclusions`) to use the configured File Threat Protection exclusions during the scan.

By default, both settings are enabled.

> In order to optimize the operation of scan tasks, it is recommended to add the path with snapshots mounted by the system in the read-only mode to the exclusions for the systems with the btrfs file system and enabled active snapshots. For example, for the systems based on SUSE/OpenSUSE, you can add the following exclusion for the path: `/.snapshots/*/snapshot/`.

Recommendations for the Web Threat Protection and Network Threat Protection tasks

General recommendations

Firewall of the operating system

If the system has its own network rules (or firewalld rules) with Drop policies, then for the application to work correctly, add an accept rule to allow incoming connections from the local device (loopback):

Example command for iptables

```
iptables -A INPUT -i lo -j ACCEPT
```

List of monitored network ports

Restrict the list of network ports monitored by the application. By default, the application only monitors selected network ports. If the device uses an SMB connection, make sure the default value is used:

- In the policy in the Web Console or Administration Console: in the network traffic scan settings, the **Monitor selected network ports only** option is selected.
- Locally on the device: the `MonitorNetworkPort` network traffic scan setting is set to `Selected`.

Using the application together with HAProxy

When using the application together with the HAProxy load balancer:

1. Open the /var/opt/kaspersky/kesl/common/kesl.ini configuration file, create the `[Environment]` section and add the `TcpSynInterceptDisabled=1` setting to it.

2. Restart the application:

   ```
   systemctl restart kesl
   ```

Using the application together with Kubernetes

For the Web Threat Protection and Network Threat Protection components and the Kubernetes cluster with the Calico and Cilium network plug-ins to work together, manage the `WtpFwMark`, `NtpFwMark`, `BypassFwMark`, and `BypassNflogMark` settings in the kesl.ini configuration file.

What to do if you get the "Application module integrity check failed" error

Recommendations for Web Threat Protection

Certificate verification policy

By default, the Web Threat Protection component decrypts and scans network traffic sent over encrypted connections. When doing so, the component can use the internet for the verification and download missing chains required to verify the certificate.

If the device does not have direct internet access, do one of the following:

- Select a local certificate validation method in the network traffic scan settings:

  - In the policy using the Web Console or Administration Console: set **Certificate verification policy** to **Local check**.

  - Locally on the device using the command line:

    ```
    kesl-control --set-net-settings CertificateVerificationPolicy=LocalCheck
    ```

  The application will not use the internet to verify certificates.

- Configure internet access via a proxy server:
  - In a policy, using the Web Console or Administration Console: Configure proxy settings.
  - Locally on the device using the command line:

    Enable the use of a proxy server with authentication

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<user name>:<password>@<IP address of the proxy server>:<port number>
    ```

    Enable the use of a proxy server without authentication

    ```
    kesl-control --set-app-settings UseProxy=Yes ProxyServer=<connection protocol>://<IP address of the proxy server>:<port number>
    ```

Recommendations for Network Threat Protection

Compatibility with REDIRECT rules

To ensure the compatibility of interception rules of the Network Threat Protection component with REDIRECT rules (for example, redirection from port 443 to 8443):

1. Delete the rule:

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
   ```

2. Replace it with the following rules:

   ```
   iptables -t nat -A PREROUTING -p tcp -m tcp --dport 443 -m mark ! --mark 0x400/0x400 -j REDIRECT --to-ports 8443
   iptables -t nat -A OUTPUT -p tcp --dport 443 -m mark --mark 0x400/0x400 -m addrtype ! --src-type LOCAL -j DNAT --to-destination :8443
   ```

Recommendations for Behavior Detection

We recommend excluding from scanning the activity of processes that are most frequently scanned by the Behavior Detection component.

To find out which processes are started most frequently, run the following command:

```
kesl-control --get-statistic --processes
```

This command outputs the list of processes whose starts Kaspersky Endpoint Security detects most frequently, and the start count for these projects.

You can configure exclusions in a policy using the Web Console or Administration Console, or locally on the device using the command line.

By default, only the specified process is excluded from the scan; Behavior Detection continues to scan the child processes of an excluded process.

Examples of configuring exclusions on the command line

Exclude the activity of my_program1 and my_program2 from scanning

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0001.ProgramPath=/bin/my_program2
```

Exclude the activity of my_program1 and its child processes from scanning

```
kesl-control --set-settings 20 UseTrustedPrograms=Yes TrustedPrograms.item_0000.ProgramPath=/bin/my_program1
TrustedPrograms.item_0000.ApplyToDescendants=Yes
```

Interoperability with Kaspersky solutions

The Kaspersky Endpoint Security application supports interoperability with some Kaspersky solutions. For optimal interoperability of the applications, follow the guidelines in this section.

Kaspersky Security Center Linux

When using Kaspersky Endpoint Security for Linux together with Kaspersky Security Center Linux, we recommend using the settings described in this article.

Recommended settings

Application component	Recommended component state	Recommendations
File Threat Protection	Enabled	Add protection exclusions: • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent` • `/var/lib/postgresql/<PostgreSQL version>`
Malware Scan	Enabled	
Removable drives scan	Disabled	–
Behavior Detection	Enabled	Use the default settings.
Network Threat Protection	Enabled	Select the eBPF network traffic interception mode `NetInterceptorMode=UseEBPF`
Web Threat Protection	Enabled	Use the default settings.
Anti-Cryptor	Disabled	–
Container Scan	Disabled	–
Inventory	Disabled	–
Device Control	Disabled	–
Application Control	Disabled	–
Firewall	Disabled	–
Web Control	Disabled	–

Application component	Recommended component state	Recommendations
System Integrity Monitoring	Enabled	Add scan scopes: • /etc • /opt/kaspersky/kesl/ • /opt/kaspersky/ksc64
System Integrity Check	Disabled	–
Endpoint Detection and Response Expert (on-premises)	Enabled	Use the default settings.
Endpoint Detection and Response Expert (cloud)	Disabled	–
Managed Detection and Response	Enabled	Use the default settings.
Network Detection and Response (KATA)	Disabled	–
Integration with KUMA	Disabled	–
Sandbox	Disabled	–
Response actions	Some limitations apply	For response actions, you cannot exclude objects required by Kaspersky Endpoint Security for Linux, as well as critical system objects. When initiating response actions, make sure that they do not disrupt the system and the applications that you use.
Graphical interface	Not set	–
Kaspersky Endpoint Security for Linux management web plug-in	Installed	Use the default settings.
Kaspersky Endpoint Security for Linux MMC management plug-in	Installed	Use the default settings.
Network Agent	Installed	Use the default settings.
File operation interception mechanism	System interception mechanism based on fanotify	Use the default settings.
System event telemetry source	eBPF+auditd	`TelemetrySource=Default`
Exploit Prevention	Disabled	–
Using Kaspersky Security Network	Enabled	Use the default settings.
Mail Threat Protection	Enabled	Use the default settings.
BadUSB Attack Prevention	Disabled	–
Global exclusions	Configured	If you install Kaspersky Security Center using quick install script, add mount points to exclusions: `/var/lib/postgresql/<PostgreSQL version>/main` where `<PostgreSQL version>` is the number of the PostgreSQL DBMS version that you use.

Network Detection and Response (KATA)

When using Kaspersky Endpoint Security for Linux together with Network Detection and Response (KATA), we recommend using the settings described in this article.

Also review the documentation of the Kaspersky Anti Targeted Attack (KATA) Platform solution.

Settings for Kaspersky Endpoint Security for Linux on servers with the Sensor component

Recommended settings for Sensor servers

Application component	Recommended component state	Recommendations
File Threat Protection	Enabled	Add protection exclusions: • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*preprocessor_icap*]/tmp/content` • `[container-name:*preprocessor_span*]/tmp/suricata` • `[container-name:*preprocessor_span*]/mnt/kaspersky/nta` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*]/var/log/kaspersky`
Malware Scan	Disabled	–
Removable drives scan	Disabled	–
Behavior Detection	Enabled	Use the default settings.
Network Threat Protection	Disabled	–
Web Threat Protection	Disabled	–
Anti-Cryptor	Disabled	–
Container Scan	Enabled	Enable Container Monitoring to scan running containers and namespaces in real time `NamespaceMonitoring=Yes`
Inventory	Disabled	–
Device Control	Disabled	–
Application Control	Disabled	–
Firewall	Disabled	–
Web Control	Disabled	–
System Integrity Monitoring	Disabled	–
System Integrity Check	Disabled	–
Endpoint Detection and Response Expert (on-premises)	Disabled	–
Endpoint Detection and Response Expert (cloud)	Disabled	–
Managed Detection and Response	Disabled	–
Network Detection and Response (KATA)	Disabled	–
Integration with KUMA	Disabled	–

Application component	Recommended component state	Recommendations
Sandbox	Disabled	–
Response actions	Disabled	–
Graphical interface	Not set	–
Network Agent	Installed	Use the default settings.
File operation interception mechanism	System interception mechanism based on fanotify	Use the default settings.
System event telemetry source	eBPF+auditd	`TelemetrySource=Default`
Exploit Prevention	Disabled	–
Using Kaspersky Security Network	Enabled	Use the default settings.
Mail Threat Protection	Disabled	–
BadUSB Attack Prevention	Disabled	–
Trace files	–	Change the directory for trace files to a directory outside the `/var/log/kaspersky` directory. For example, use the `/var/log/kesl` directory.
Global exclusions	Configured	Exclude the following mount points: • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` The exclusion of the tmp/apttmp/*, /tmp/suricata/*, /tmp/traffic/* and /tmp/apt_certs/* mount points applies to NDR (KATA) servers version 8.0 and earlier. • `/varog/kaspersky` • `/var/opt/kaspersky` • `/data` • `/data/volumes/dumps`

Settings for Kaspersky Endpoint Security for Linux on servers with the Central Node component

Recommended settings for Central Node servers

Application component	Recommended component state	Recommendations
File Threat Protection	Enabled	Add protection exclusions: • `[container-name:*edr_synchronizer*]/tmp/` • `[container-name:*ids_alert_syncer*]/tmp/` • `[container-name:kata_product_main_1_kata_scanner]/storage` • `[container-name:kata_product_main_1_postgresql_server]/var/lib/postgresql` • `[container-name:kata_product_main_1_clickhouse]/var/lib/clickhouse` • `[container-name:*kata_scanner*]/storage/data/var/opt/kaspersky/apt-collector/spool` • `[container-name:*kata_scanner*]/var/opt/kaspersky/apt-agents` • `[container-name:*kata_scanner*]/var/lib/nginx/body` • `[container-name:*kata_scanner*]/apt_spool` • `[container-name:*kata_scanner*]/tmp/` • `[container-name:*kafka*]/tmp/` • `[container-name:*ksn_proxy*]/tmp/` • `[container-name:*preprocessor_smtp*]/tmp/` • `[container-name:*preprocessor_pop*]/tmp/` • `[container-name:*preprocessor_icap*]/tmp/` • `[container-name:*preprocessor_span*]/tmp/` • `[container-name:*sandbox_scan*]/tmp/` • `[container-name:*statistics_clickhouse_importer*]/tmp/` • `[container-name:*updates_consistency_checker*]/tmp/` • `[container-name:*web_backend*]/tmp/` • `[container-name:*]/var/opt/kaspersky` • `/tmp/` • `/var/log/kaspersky`
Malware Scan	Disabled	–
Removable drives scan	Disabled	–
Behavior Detection	Enabled	Use the default settings.
Network Threat Protection	Disabled	–
Web Threat Protection	Disabled	–
Anti-Cryptor	Disabled	–
Container Scan	Enabled	Enable Container Monitoring to scan running containers and namespaces in real time `NamespaceMonitoring=Yes`
Inventory	Disabled	–
Device Control	Disabled	–
Application Control	Disabled	–
Firewall	Disabled	–
Web Control	Disabled	–
System Integrity Monitoring	Disabled	–
System Integrity Check	Disabled	–
Endpoint Detection and Response Expert (on-premises)	Disabled	–

Application component	Recommended component state	Recommendations
Endpoint Detection and Response Expert (cloud)	Disabled	–
Managed Detection and Response	Disabled	–
Network Detection and Response (KATA)	Disabled	–
Integration with KUMA	Disabled	–
Sandbox	Disabled	–
Response actions	Disabled	–
Graphical interface	Not set	–
Network Agent	Installed	Use the default settings.
File operation interception mechanism	System interception mechanism based on fanotify	Use the default settings.
System event telemetry source	eBPF+auditd	`TelemetrySource=Default`
Exploit Prevention	Disabled	–
Using Kaspersky Security Network	Enabled	Use the default settings.
Mail Threat Protection	Disabled	–
BadUSB Attack Prevention	Disabled	–
Trace files	–	Change the directory for trace files to a directory outside the `/var/log/kaspersky` directory. For example, use the `/var/log/kesl` directory.
Global exclusions	Configured	Add mount points to exclusions: • `/apt_spool` • `/storage` • `/var/lib/postgresql` • `/var/lib/clickhouse` • `/tmp/apttmp/*` • `/tmp/suricata/*` • `/tmp/traffic/*` • `/tmp/apt_certs/*` The exclusion of the tmp/apttmp/*, /tmp/suricata/*, /tmp/traffic/* and /tmp/apt_certs/* mount points applies to NDR (KATA) servers version 8.0 and earlier. • `/var/log/kaspersky` • `/var/opt/kaspersky` • `/data`

Kaspersky Unified Monitoring and Analysis Platform

When using Kaspersky Endpoint Security for Linux together with Kaspersky Unified Monitoring and Analysis Platform, we recommend using the settings described in this article.

Application component	Recommended component state	Recommendations
File Threat Protection	Enabled	Add protection exclusions: • `/opt/kaspersky/kuma` • `/opt/kaspersky/klnagent/sbin/klnagent` • `/opt/kaspersky/klnagent64/sbin/klnagent`
Malware Scan	Disabled	–
Removable drives scan	Disabled	–
Behavior Detection	Enabled	Exclude the process from scanning `/opt/kaspersky/kuma`
Network Threat Protection	Enabled	Disable blocking of the compromised device `BlockAttackingHosts=No`
Web Threat Protection	Disabled	–
Anti-Cryptor	Disabled	–
Container Scan	Disabled	–
Inventory	Disabled	–
Device Control	Disabled	–
Application Control	Disabled	–
Firewall	Disabled	–
Web Control	Disabled	–
System Integrity Monitoring	Disabled	–
System Integrity Check	Disabled	–
Endpoint Detection and Response Expert (on-premises)	Disabled	–
Endpoint Detection and Response Expert (cloud)	Disabled	–
Managed Detection and Response	Disabled	–
Network Detection and Response (KATA)	Disabled	–
Integration with KUMA	Disabled	–
Sandbox	Disabled	–
Response actions	Disabled	–
Graphical interface	Not set	–
Network Agent	Installed	Use the default settings.
File operation interception mechanism	System interception mechanism based on fanotify	Use the default settings.
System event telemetry source	eBPF+auditd	`TelemetrySource=Default`
Exploit Prevention	Disabled	–
Using Kaspersky Security Network	Enabled	Use the default settings.
Mail Threat Protection	Disabled	–
BadUSB Attack Prevention	Disabled	–

Application components reference

Commands for managing Kaspersky Endpoint Security

In the command line, Kaspersky Endpoint Security is managed using Kaspersky Endpoint Security management commands.

You can view the help on management commands by running:

```
kesl-control --help <prefix of command group>
```

where `<prefix of command group>` can take the following values:

- `-A`: commands for managing Application Control
- `-B`: commands for managing Backup
- `-C`: commands for managing general container scan settings
- `-D`: commands for managing Device Control
- `-E`: commands for viewing current application events
- `-F`: commands for Firewall Management
- `-H`: commands for managing devices blocked by Anti-Cryptor and Network Threat Protection
- `-J`: commands for managing the obtaining of system performance metrics
- `-L`: commands for managing license keys
- `-M`: commands for managing the integration settings of the Kaspersky Endpoint Security application with Kaspersky Unified Monitoring and Analysis Platform
- `-N`: commands for managing encrypted connections scan settings
- `-Q`: commands for managing the Quarantine
- `-R`: commands for managing the settings of Kaspersky Endpoint Security integration with Kaspersky Endpoint Detection and Response (KATA), Kaspersky Network Detection and Response (KATA), Kaspersky Endpoint Detection and Response Expert (cloud), and Kaspersky Endpoint Detection and Response Optimum
- `-S`: statistical commands.
- `-T`: commands for managing application tasks and settings
- `-U`: commands for managing users and roles
- `-V`: application commands in Light Agent mode

- `-W`: commands for displaying events from the application event log
- `-X`: commands for managing the integration settings of the Kaspersky Endpoint Security application with Sandbox

In the bash shell, you can enable autocompletion for the kesl-control commands.

```
Enable autocompletion for the kesl-control command in the current bash session
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

```
Enable autocompletion for all new bash sessions
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~/.bashrc
```

Commands for managing license keys

The `-L` prefix indicates that the command belongs to the group of commands used to manage license keys.

> Commands for adding or removing license keys can be used if the application is running in Standard mode or in EDR Agent mode. If the application is used in Light Agent mode, key management commands return an error.

kesl-control --add-active-key

The command lets you add an active license key to the application using a key file or activation code.

You can use this command to add keys for activating the application keys for activating components that are not covered by your license. You do not need to specify the type of the key in the command.

```
Add a license key using a key file
kesl-control [-L] --add-active-key <key file path>
```

```
Add a license key using an activation code
kesl-control [-L] --add-active-key <activation code>
```

Where:

`<key file path>` is the path to the key file. If the key file is located in the current directory, it is sufficient to specify only the file name.

`<activation code>` is the activation code.

```
Example of adding a key using the /home/test/00000001.key file as the active key
kesl-control --add-active-key /home/test/00000001.key
```

kesl-control --add-reserve-key

The command lets you add a reserve license key to the application using a key file or activation code.

You can use this command to add keys for activating the application keys for activating components that are not covered by your license. You do not need to specify the type of the key in the command.

> If an active key has not yet been added to the application on the device, the command fails.

Add a reserve license key using a key file

```
kesl-control [-L] --add-reserve-key <key file path>
```

Add a reserve license key using an activation code

```
kesl-control [-L] --add-reserve-key <activation code>
```

Where:

`<key file path>` is the path to the key file. If the key file is located in the current directory, it is sufficient to specify only the file name.

`<activation code>` is the activation code.

Example of adding a reserve key using the /home/test/00000002.key file

```
kesl-control --add-reserve-key /home/test/00000002.key
```

kesl-control --remove-active-key

This command lets you remove an active license key.

```
Delete the active EDR Optimum license key
```

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

```
Delete the active KUMA license key
```

```
kesl-control [-L] --remove-active-key [--kuma]
```

```
Delete the active MDR license key
```

```
kesl-control [-L] --remove-active-key [--mdr]
```

```
Delete the active EDR Expert (on-premises) license key
```

```
kesl-control [-L] --remove-active-key [--edr-kata]
```

```
Delete the active EDR Expert (cloud) license key
```

```
kesl-control [-L] --remove-active-key [--cxdr]
```

```
Delete the active KWSM license key
```

```
kesl-control [-L] --remove-active-key [--khcs]
```

Where:

`--edr-optimum` – delete the active EDR Optimum license key.

`--kuma` – remove the active KUMA license key.

`--mdr` – remove the active MDR license key.

`--edr-kata` – remove the active EDR Expert (on-premises) license key.

`--cxdr` – remove the active EDR Expert (cloud) license key.

`--khcs` – remove the active KWSM license key.

If you do not specify the `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr`, or `--khcs` option in the command line, the command deletes the active key with which your application is activated.

kesl-control --remove-reserve-key

This command lets you remove a reserve license key.

```
Delete the reserve EDR Optimum license key
```

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

```
Delete the reserve KUMA license key
```

```
kesl-control [-L] --remove-reserve-key [--kuma]
```

```
Delete the reserve MDR license key
```

```
kesl-control [-L] --remove-reserve-key [--mdr]
```

```
Delete the reserve EDR Expert (on-premises) license key
```

```
kesl-control [-L] --remove-reserve-key [--edr-kata]
```

```
Delete the reserve EDR Expert (cloud) license key
```

```
kesl-control [-L] --remove-reserve-key [--cxdr]
```

```
Delete the reserve KWSM license key
```

```
kesl-control [-L] --remove-reserve-key [--khcs]
```

Where:

`--edr-optimum` – delete the reserve EDR Optimum license key.

`--kuma` – remove the reserve KUMA license key.

`--mdr` – remove the reserve MDR license key.

`--edr-kata` – remove the reserve EDR Expert (on-premises) license key.

`--cxdr` – remove the reserve EDR Expert (cloud) license key.

`--khcs` – remove the reserve KWSM license key.

If you do not specify the `--edr-optimum`, `--kuma`, `--mdr`, `--edr-kata`, `--cxdr`, or `--` option in the command line, the command removes the reserve key from the application.

kesl-control -L --query

The command outputs information about the license that was used to activate the application and the license keys currently in use.

```
kesl-control -L --query [--json]
```

Where:

`--json`: output data in JSON format.

kesl-control --load-mdr-blob

The command lets you upload a BLOB file to the device, which can be used for integration with Kaspersky Managed Detection and Response. You can find the BLOB file in the ZIP archive of the MDR configuration file.

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB file>
```

kesl-control --remove-mdr-blob

The command lets you remove the BLOB file, which is used for integration with Kaspersky Managed Detection and Response, from the device.

```
kesl-control [-L] --remove-mdr-blob
```

Commands for managing users and roles

The -U prefix indicates that the command belongs to the group of commands for managing users and roles.

Managing user roles

```
Display a list of users and roles
kesl-control [-U] --get-user-list
```

```
Assign a role to the specified user
kesl-control [-U] --grant-role <role> <user>
```

```
Revoke a user role
kesl-control [-U] --revoke-role <role> <user>
```

Where:

`<user>` is a user or user group name.

`<role>` is a user or user group role.

Password protection settings

You can use commands to manage Password protection.

```
Enable or disable Password protection
kesl-control --set-permission-manager-settings Enabled=<Yes|No>
```

```
View the current Password protection settings
kesl-control --get-permission-manager-settings
```

```
Edit the permissions of a user or group
kesl-control --set-permissions <user> [--group] <permissions>=<Yes|No> [--file <file name>] [--json]
```

```
View current permissions for a user or group
kesl-control --get-permissions <user> [--group] [--file <file name>] [--json]
```

```
Remove a user or group of users for which permissions are configured
kesl-control --remove-permissions <user> [--group]
```

Where:

`<user>` is a user or user group name.

`<permissions>` is for custom permissions.

`--group` applies the setting to a group of users. If this option is not specified, the setting is applied to an individual user.

`--file <path to file>` saves or exports settings into a configuration file. If this option is not specified, the result of the command is written to standard output.

`--json` is specified to output the settings in JSON format.

Managing the policy on the device

To disable the policy on a device, the user needs the Disable Kaspersky Security Center policy permission.

If the user has disabled the policy on the device, the policy becomes active again after the device or Kaspersky Endpoint Security is restarted.

Disable the policy on the device

```
kesl-control --disable-policy
```

Apply the policy to the device

```
kesl-control --enable-policy
```

Managing application tasks and settings

The `-T` prefix indicates that the command belongs to the group of commands for managing application settings and tasks.

The `-C` prefix indicates that the command belongs to the group of commands for managing Container Scan settings.

The `-N` prefix indicates that the command belongs to the group of commands for managing network traffic scan settings.

kesl-control --export-settings

This command outputs all application settings to the console or exports to a configuration file. These include general container scan settings, encrypted connections scan settings, general application settings, and task settings.

```
kesl-control [-T] --export-settings [--file <path to file>] [--json]
```

Where:

`--file <path to file>` is the full path to the configuration file to which you want to save application settings.

`--json` is specified to output the settings in JSON format.

kesl-control --import-settings

> Grant access to the configuration file only to trusted users. Before importing settings into the application, verify the paths to directories, configuration files, executable files, and the quarantine. Do not import configuration files from untrusted sources. Compromising the configuration file could affect the security, integrity, or functionality of the infrastructure of your organization, as well as user data.

This command imports all application settings from a configuration file, including general container scan settings, encrypted connections scan settings, general application settings, and task settings.

```
kesl-control [-T] --import-settings --file <path to configuration file> [--json]
```

Where:

`--file <path to file>` is the full path to the configuration file from which you want to import application settings.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

kesl-control --update-application

This command installs a downloaded application module update.

> The command cannot be run if the application is being used in Light Agent mode

```
kesl-control [-T] --update-application
```

Commands for managing general application settings

kesl-control --get-app-settings

The command outputs the current values of the general application settings to the console or a configuration file.

```
kesl-control [-T] --get-app-settings [--file <path to file>] [--json]
```

Where:

`--file <path to file>` is the path to the configuration file to which you want to output the general settings of the application. If you do not specify the `--file` option, settings will be output to the console.

If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, no configuration file will be generated.

`--json` is specified to output the settings in JSON format.

kesl-control --set-app-settings

This command configures the general application settings via command options or by importing settings from a configuration file.

```
Specify settings using command line options:
```

```
kesl-control [-T] --set-app-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

```
Specify settings using a configuration file:
```

```
kesl-control [-T] --set-app-settings --file <path to file> [--json]
```

Where:

`<setting name>=<setting value>` is the name and value of a general application setting.

`--file <path to file>` is the full path to the configuration file from which you want to import application settings.

`--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

Commands for managing task settings

kesl-control --get-settings

This command outputs the current settings for a specified task to the console or a configuration file.

```
kesl-control [-T] --get-settings <task ID|name> [--file <path to file>] [--json]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`--file <path to file>` is the path to the configuration file to which you want to output the task settings. If you do not specify the `--file` option, settings will be output to the console.

If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, no configuration file will be generated.

`--json` is specified to output the settings in JSON format.

kesl-control --set-settings

This command defines the settings for a specified task via command options or by importing settings from a configuration file.

```
Specify settings using command line options:

kesl-control [-T] --set-settings <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

```
Specify settings using a configuration file:

kesl-control [-T] --set-settings <task ID/name> --file <path to file> [--json]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`<setting name>=<setting value>` is the name and value of one task setting.

`--add-path <path>` adds a path to a directory with objects to be scanned.

`--del-path <path>` removes a path to a directory with objects to be scanned.

`--add-exclusion <path>` adds a path to a directory with objects to be excluded from scanning.

`--del-exclusion <path>` removes a path to a directory with objects to be excluded from scanning.

`--file <path to file>` is the full path to the configuration file from which you want to import the task settings.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

kesl-control --set-to-default

The command restores the default settings for the specified task.

```
kesl-control [-T] --set-settings <task ID|name> --set-to-default
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

kesl-control --get-schedule

The command outputs the current schedule of the specified task to the console or a configuration file.

```
kesl-control [-T] --get-schedule <task ID|name> [--file <path to file>] [--json]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`--file <path to file>` is the path to the configuration file to which you want to output the task schedule settings. If you do not specify the `--file` option, settings will be output to the console.

If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, no configuration file will be generated.

`--json` is specified to output the settings in JSON format.

kesl-control --set-schedule

The command defines a schedule for the specified task via command options or by importing settings from a configuration file.

```
Specify settings using command line options:
```

```
kesl-control [-T] --set-schedule <task ID|name> <setting name>=<setting value> [<setting name>=<setting value>]
```

```
Specify settings using a configuration file:
```

```
kesl-control [-T] --set-schedule <task ID|name> --file <path to file> [--json]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`<setting name>=<setting value>` is the name and value of one task schedule setting.

`--file <path to file>` is the full path to the configuration file from which you want to import the task schedule settings.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

Commands for managing tasks

kesl-control --get-task-list

This command outputs a list of existing tasks.

```
kesl-control [-T] --get-task-list [--json]
```

Where:

`--json` is specified to output the settings in JSON format.

The following information will be displayed for each task:

- `Name`: the task name
- `ID`: the task ID
- `Type`: the task type
- `State`: the current state of the task

> If the Kaspersky Security Center policy prohibits users from viewing and editing local tasks, information about the `Scan_My_Computer`, `Critical_Areas_Scan`, `Container_Scan`, `Inventory_Scan`, `Update`, and `Rollback` tasks is not available.

kesl-control --get-task-state

This command outputs the status of the specified task.

```
kesl-control [-T] --get-task-state <task ID|name> [--json]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`--json` is specified to output the settings in JSON format.

Application tasks can take the following states:

- `Started` – Task is running.
- `Starting` – Task is being launched.

- `Stopped` – Task has been stopped.
- `Stopping` – Task is stopping.

Tasks of the `ODS`, `ODFIM`, and `InventoryScan` types can also have one of the following states:

- `Pausing` – Task is pausing.
- `Suspended` – Task is suspended.
- `Resuming` – Task is resuming.

kesl-control --create-task

This command creates a task of the specified type with the default settings or settings specified in a configuration file.

Only user tasks can be created. Predefined tasks cannot be created.

Depending on the mode of the application, you can create the following types of user tasks:

- Standard mode: `ODS`, `Update`, `Rollback`, `ODFIM`, `ContainerScan`, and `InventoryScan`.
- Light Agent mode: `ODS`, `ODFIM`, `ContainerScan`, and `InventoryScan`.

```
Create a task with the default settings
kesl-control [-T] --create-task <task name> --type <task type>
```

```
Create a task with the settings from a configuration file
kesl-control [-T] --create-task <task name> --type <task type> [--file <path to file>] [--json]
```

Where:

`<task name>` is a name you specified for a new task.

`<task type>` specifies the type of task that you want to create.

`--file <path to file>` is the full path to the configuration file with the settings that will be used for creating the task.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

kesl-control --delete-task

This command deletes a task.

Only user tasks can be deleted. Predefined tasks cannot be deleted.

```
kesl-control [-T] --delete-task <task ID|name>
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

kesl-control --start-task

This command starts a task.

You can start and stop all predefined tasks and user tasks except tasks of the `License` type.

```
kesl-control [-T] --start-task <task ID|name> [-W] [--progress]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`-W`: enable current events output.

`--progress`: display task progress.

```
Example of running a task with ID 1 and enabling the display of current events associated with the task
kesl-control --start-task 1 -W
```

If an error occurs when starting a task and the task does not start, then after the application is restarted, an attempt is made to start the task again.

kesl-control --stop-task

This command stops a task.

You can start and stop all predefined tasks and user tasks except tasks of the `License` type.

```
kesl-control [-T] --stop-task <task ID|name> [-W]
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

`-W`: enable current events output.

kesl-control --suspend-task

This command pauses a task.

You can only suspend `ODS`, `ODFIM`, and `InventoryScan` tasks.

```
kesl-control [-T] --suspend-task <task ID|name>
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

kesl-control --resume-task

This command resumes a task.

You can only resume `ODS`, `ODFIM`, and `InventoryScan` tasks.

```
kesl-control [-T] --resume-task <task ID|name>
```

Where:

`<task ID|name>` is the ID assigned to the task at the time of its creation, or the name of the task on the command line.

kesl-control --scan-file

This command creates and runs a custom scan task.

```
kesl-control [-T] --scan-file <path> [--action <action>]
```

Where:

`<path>` is the path to the file or directory that you want to scan. You can specify multiple paths by separating them with a space.

`--action <action>` is the action that you want application to perform on infected objects. If you do not specify the `--action` option, the application performs the recommended action.

kesl-control --scan-container

This command creates and runs a custom container or image scan task.

```
kesl-control [-T] --scan-container <ID|name[:tag]>
```

Where:

`<ID|name[:tag]>` is the name or ID of the container or image. You can use masks to scan several objects.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Commands for managing general Container Scan settings

kesl-control --get-container-settings

The command outputs the current general container scan settings to the console or a configuration file.

```
kesl-control [-C] --get-container-settings [--file <path to file>] [--json]
```

Where:

`--file <path to file>` is the path to the configuration file to which you want to output the general settings of Container Scan. If you do not specify the `--file` option, settings will be output to the console.

If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, no configuration file will be generated.

`--json` is specified to output the settings in JSON format.

kesl-control --set-container-settings

The command configures the general container scan settings with command options or by importing settings from a configuration file.

```
Specify settings using command line options:

kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

```
Specify settings using a configuration file:

kesl-control [-C] --set-container-settings --file <path to file> [--json]
```

Where:

`<setting name>=<setting value>` is the name and value of a general Container Scan setting.

`--file <path to file>` is the full path to the configuration file from which you want to import the general Container Scan settings.

`--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

Commands for managing network traffic scan settings

The `-N` prefix indicates that the command belongs to the group of commands for managing network traffic scan settings.

kesl-control -N --query

The command outputs lists of exclusions from encrypted connections scanning:

- a list of exclusions added by the user;
- a list of exclusions added by the application;
- list of exclusions received from the application databases.

```
Display a list of exclusions added by the user
kesl-control -N --query user
```

```
Display a list of exclusions added by the application
kesl-control -N --query auto
```

```
Display a list of exclusions received from the application databases
kesl-control -N --query kl
```

kesl-control --clear-web-auto-excluded

This command clears the list of domains that the application has automatically excluded from scanning.

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

This command outputs the current network traffic scan settings to the console or a configuration file.

```
kesl-control [-N] --get-net-settings [--file <path to file>] [--json]
```

Where:

`--file <path to file>` is the path to the configuration file to which you want to output network traffic scan settings. If you do not specify the `--file` option, settings will be output to the console.

If you specify the name of a file without its path, the file will be created in the current directory. If a file already exists in the specified path, it will be overwritten. If the specified directory does not exist, no configuration file will be generated.

`--json` is specified to output the settings in JSON format.

kesl-control --set-net-settings

This command configures the network traffic scan settings with command options or by importing settings from a configuration file.

```
Specify settings using command line options:
```

```
kesl-control [-N] --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

```
Specify settings using a configuration file:
```

```
kesl-control [-N] --set-net-settings --file <path to file> [--json]
```

Where:

`<setting name>=<setting value>` is the name and value of a network traffic scan setting.

`--file <path to file>` is the full path to the configuration file from which you want to import network traffic scan settings.

`--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

kesl-control --list-certificates

This command outputs a list of trusted root certificates.

```
kesl-control [-N] --list-certificates
```

kesl-control --add-certificate

This command adds a certificate to the list of trusted root certificates.

```
kesl-control [-N] --add-certificate <path to certificate>
```

Where:

`<path to certificate>` is the path to the certificate file that you want to add (in PEM or DER format).

kesl-control --remove-certificate

This command removes a certificate from the list of trusted root certificates.

```
kesl-control [-N] --remove-certificate <certificate subject>
```

kesl-control --add-bypass-endpoints

This command lets you add traffic interception exclusion.

```
kesl-control [-N] --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Where:

`<in|out>` is the direction of traffic in the excluded connection, outbound or inbound.

`<remote IP address>` is the IPv4 or IPv6 address of the remote device. If you exclude inbound traffic from interception, traffic coming from the specified IP address is excluded. If you exclude outbound traffic from interception, traffic going to the specified IP address is excluded.

`<destination port>` is a port on the protected device (exclusion for inbound traffic) or a port on the remote device (exclusion for outbound traffic). Traffic to this port is excluded from interception.

kesl-control --list-bypass-endpoints

This command lets you view the list of configured traffic interception exclusions.

```
kesl-control [-N] --list-bypass-endpoints
```

kesl-control --remove-bypass-endpoints

This command lets you remove a traffic interception exclusion.

```
kesl-control [-N] --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

Where:

`<in|out>` is the direction of traffic in the excluded connection, outbound or inbound.

`<remote IP address>` is the IPv4 or IPv6 address of the remote device whose traffic is excluded from interception (depending on the direction of traffic).

`<destination port>` is a port on the protected device (exclusion for inbound traffic) or a port on the remote device (exclusion for outbound traffic).

Status and protection monitoring

Statistics commands

The -S prefix indicates that the command belongs to the statistics command group.

kesl-control --app-info

This command outputs information about the application.

```
kesl-control [-S] --app-info [--json] [--check-permissions]
```

Where:

`--json` is specified to output the settings in JSON format.

`--check-permissions` displays paths to application directories with incorrectly configured permissions.

kesl-control --supported-tech-info

This command displays a list of application functions, information about their status (used or not used), and the Linux technologies that these application features are implemented with.

```
kesl-control [-S] --supported-tech-info [--json]
```

Where:

`--json`: output features in JSON format.

kesl-control --get-statistic

The command allows you to display statistics about the operation of the application and the list of mount points found on the device.

```
kesl-control [-S] --get-statistic [--files] [--processes] [--mountpoints]
```

Where:

`--files`: statistics of files most frequently scanned by the File Threat Protection component, and the number of times the component accesses these files.

`--processes`: statistics of process starts most frequently detected by Kaspersky Endpoint Security, and the number of such starts.

> Excluding processes from scanning by the Behavior Detection component does not remove these processes from statistics, but it improves the performance of the Kaspersky Endpoint Security application.

`--mountpoints`: list of mount points. In the output, paths to mount points are sorted as follows:

- Static, system, service and other mount points
- Mounted snap packages and mount points in their namespaces
- Mount points created by the Docker container management system

You can specify one or more options in any combination or no options at all. If you do not specify any options, the application displays three lists: statistics on the most frequently scanned files, statistics on the most frequently started processes, and the list of mount points found on the device.

kesl-control --omsinfo

This command creates a JSON file for integration with Microsoft Operations Management Suite.

```
kesl-control [-S] --omsinfo --file <path to file>
```

Command for displaying events

The `-W` prefix indicates a command for displaying events from the application event log.

kesl-control -W

This command enables the display of current application events. The command returns the name of the event and additional information about the event. You can use the command to display all current application events or only events associated with a currently running task.

```
kesl-control -W [--query "<filter conditions>"]
```

Where:

`<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operation> '<value>'` format combined using the logical operator `and` to output certain current events.

Commands for managing application events

The -E prefix indicates that the command belongs to the group of commands used for managing application events.

kesl-control -E

This command outputs information about all events in the application event log. You can use the `less` command to navigate through the list of displayed events.

```
kesl-control -E
```

kesl-control -E --query

This command outputs information about events from the application event log. You can use the `less` command to navigate through the list of displayed events. You can use a filter to output specific events or output a list of events to a file.

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--file <path to file>] [--
json] [--reverse]
```

Where:

`<database file>` is the full path to the event log database file to output events from. By default, the application saves information about events to the database at /var/opt/kaspersky/kesl/private/storage/events.db. The location of the database is determined by the `EventsStoragePath` general application setting.

`<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operator> '<value>'` format combined using the logical operator `and` to restrict the results of the query.

`<number>` is the number of the latest events in the selection (that is, the number of records counting from the end of the selection) that you want to output.

`--file <path to file>` is the full path to the file to output events to. If you specify the name of a file without specifying its path, the file will be created in the current directory. If a file with the specified name already exists in the specified path, it will be overwritten. If the specified directory cannot be found on the disk, file will not be created.

If you do not specify the `--file` option, the list of events will be output to the console.

`--json`: output events in JSON format.

`--reverse`: display events in reverse order (from the newest event at the top to the oldest at the bottom).

Command for managing system performance metrics

kesl-control --export-metrics

This command allows to configure the obtaining of operating system performance metrics.

```
kesl-control [-J] --export-metrics [--period <interval in seconds between exports>|--interactive]
```

Where:

`--period` enables periodic output of results.

`<interval in seconds between exports>` specifies how often the command results are output to the command line console (in seconds)

`--interactive` enables interactive output (on the **Enter** key being pressed).

Security Controls

Commands for managing Device Control

The -D prefix indicates that the command belongs to the group of commands to manage Device Control.

Managing Device Control settings

```
View the current Device Control settings
kesl-control --get-settings 15 [--file <path to file>] [--json]
```

```
Modify the Application Control settings
kesl-control --set-settings 15 [<setting>=<value>] [--file <path to file>] [--json]
```

Where:

`<setting>=<value>` specifies a Device Control setting and its value.

--file <path to file> saves or exports settings into a configuration file. If this option is not specified, the result of the command is written to standard output.

`--json`: output data in JSON format.

Managing devices

```
View the list of connected devices
kesl-control [-D] --get-device-list [--all] [--json] [--export <file>]
```

Where:

`--all` lists all connected devices.

`--json` lists connected devices in JSON format.

`--export <file>` exports the list of connected devices to a JSON file. The list of connected devices is exported.

Kaspersky Endpoint Security displays the following information about connected devices:

- **Device type**. Type of the connected device. For example, `OpticalDrive` or `HardDrive`.
- **Identifier**. ID of the connected device.
- **Name**. Name of the connected device.
- **Path**. Path to the device in the sysfs virtual operating system.
- **System drive**. The setting indicates whether the connected device is a system drive (Yes or No).
- **Bus**. Connection bus. Possible values: `UnknownBus`, `USB`, `FireWire`.
- **Driver**. Name of the driver read by the sysfs virtual operating system.

Trusted devices

The command lets you view the list of trusted devices, add and remove devices from the list, and import the list of trusted devices from a file.

```
kesl-control [-D] --trusted-devices [--list] [--add <ID>] [--delete <ID>] [--merge|--add|--replace --file <file>]
```

Where:

`--list` – display the list of trusted devices.

`--add <ID>` adds a device to the list of trusted devices by device ID or device ID mask.

`--delete <ID>` removes a device from the list of trusted devices by device ID or device ID mask.

`--merge` merges the lists of trusted devices. If the current list and the imported list contain entries for a device with the same ID, the existing entries are updated. For devices that are not in the current list, entries are added.

`--add` adds the current list of trusted devices when importing. Only entries for devices not previously on the list of devices are added to the list.

`--replace` replaces the current list of trusted devices. The existing list of trusted devices is replaced with the imported list.

`--file <file>` imports a list of trusted devices from the specified file. You need to specify the full path to the JSON file.

Temporary access to a blocked device

The commands allow you to create an access request file and upload an access key to get temporary access to a blocked device:

Create an access request file

```
kesl-control [-D] --request-temporary-device-access --device-id <device ID> --access-duration <access duration> --
path <path to access request file>
```

Upload an access key

```
kesl-control [-D] --upload-temporary-device-access-key --path <access key>
```

Where:

`--device-id <device ID>` is the ID of the blocked device to which you want to gain access.

`--access-duration <access duration>` is the period of time for which you want to gain access to the device (in hours). Possible values: 1 to 100

`--path <path to access request file>` is the path to the directory in which you want to save the access request file with the .akey extension.

`--path <access key>` is the path to the file with the device access key (file with the .acode extension).

Commands for managing Application Control

The -A prefix indicates that the command belongs to the group of commands to manage Application Control.

Managing the Inventory task

```
View the list of applications detected on the client device
```

```
kesl-control [-A] --get-app-list [--json]
```

Where:

`--json`: output data in JSON format.

Viewing application categories

```
View the list of the created Application Control categories
```

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [-
-file <path to file>] [--json]
```

Where:

`<category name 1> <category name 2> ... <category name N>` are category names. If you want to view information about several categories, specify the names of the categories, separated by a space.

`--file <path to file>` saves or exports settings into a configuration file. If this option is not specified, the result of the command is written to standard output.

`--json`: output data in JSON format.

Managing application categories

To create an application category:

1. Write the list of application categories to a configuration file:

   ```
   kesl-control --set-categories --file <path to file>
   ```

2. Add application categories as follows:

```
[
   {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "GUID" : "<category ID>",
      "Include" : [ "(FilePath like <application>)", "(FileHash == <hash>)" ],
      "Name" : "<category name 2>"
   }
]
```

To specify the file path in the `Exclude` and `Include` fields, you can use masks.

3. Import the list of categories into the application:

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --
file <path to file>
```

Edit the list of Application Control categories

```
kesl-control [-A] --set-categories [--names <category name 1> <category name 2> ... <name of category N>] --file
<path to file>
```

Where:

`FilePath like <application>` is a full path to executable file of the application.

`FileHash == <hash>` is a SHA256 hash of the executable file of the application.

`<category ID>` is a unique category ID. Required setting. Enter the `GUID` without hyphens.

`<category name 1> <category name 2> ... <category name N>` are category names. Required setting.

If you want to change information about several categories, specify the names of the categories, separated by a space. If you do not specify a category name, it is not created or is deleted from the list of existing categories.

`--file <path to file>` saves or exports settings into a JSON configuration file.

Managing Application Control settings

View the current Application Control settings

```
kesl-control --get-settings 21 [--file <path to file>] [--json]
```

Modify the Application Control settings

```
kesl-control --set-settings 21 [<setting>=<value>] [--file <path to file>] [--json]
```

Where:

`<setting>=<value>` specifies an Application Control setting and its value.

`--file <path to file>` saves or exports settings into a configuration file. If this option is not specified, the result of the command is written to standard output.

`--json`: output data in JSON format.

Reset settings to default values

```
Delete a list of application categories and Application Control rules and restore the default settings
kesl-control --set-settings 21 --set-to-default
```

Useful articles

How to specify masks

You can use the * character (any sequence of characters) or the ? character (any one character) as the file or directory name mask.

You can put the * character to represent any set of characters (including an empty set) in a file or directory name that includes the / character. For example, `/dir/*/file*/` or `/dir/file*/`.

You can put a single ? character to represent any one character (including `/`) in the file or directory name.

Web Control management commands

Managing the Web Control settings

```
View the current Web Control settings
kesl-control --get-settings 26 [--file <path to file>] [--json]
```

```
Modify the Web Control settings
kesl-control --set-settings 26 [<setting>=<value>] [--file <path to file>] [--json]
```

Where:

`<setting>=<value>` is a Web Control setting and its value. You can modify any number of settings.

`--file <path to file>` saves or exports settings into a configuration file. If this option is not specified, the result of the command is written to standard output.

`--json`: output data in JSON format.

Reset settings to default values

```
Delete the configured settings and restore the default Web Control settings
```

```
kesl-control --set-settings 26 --set-to-default
```

Network connection protection

Commands used to manage blocked devices

The -H prefix indicates that the command belongs to the group of commands for managing devices blocked by Anti-Cryptor and Network Threat Protection.

kesl-control --get-blocked-hosts

The command allows you to output the list of blocked devices to the console.

```
kesl-control [-H] --get-blocked-hosts
```

kesl-control --allow-hosts

The command allows you to unblock blocked devices.

```
kesl-control [-H] --allow-hosts <address>
```

Where:

`<address>` is an IP address of a device or subnet (IPv4/IPv6, including addresses in short form). You can specify multiple IP addresses of devices or subnets by separating them with a space.

Commands for Firewall Management

The -F prefix indicates that the command belongs to the Firewall Management commands.

kesl-control --add-rule

This command adds a new network packet rule.

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

Where:

`--name <rule name>` is the name of the network packet rule.

`--action <Allow|Block>` is the action to be performed on connections specified in this network packet rule.

`--protocol <protocol>` is the protocol for which you want to monitor network activity.

`--direction <direction>` is the direction of the monitored network activity.

`--remote <remote address>:<port>` is the network address of the remote device.

`--local <local address>:<port>` is the network address of the device with Kaspersky Endpoint Security installed.

`--at <index>` is the number of the rule in the list of network packet rules. If the `--at` option is not specified or its value is larger than the number of rules in the list, the new rule is added to the end of the list.

Parameters that you do not specify values for in the command are set to their default values.

kesl-control --del-rule

This command deletes the network packet rule with the specified name or index in the list of rules.

```
Delete network packet rule by rule name
```

```
kesl-control [-F] --del-rule --name <rule name>
```

```
Delete network packet rule by rule number
```

```
kesl-control [-F] --del-rule --index <index>
```

Where:

`--name <rule name>` is the name of the network packet rule.

`--index <index>` is the number of the rule in the list of network packet rules.

kesl-control --move-rule

This command changes the execution priority of a network packet rule.

```
Change priority of network packet rule by rule name
```

```
kesl-control [-F] --move-rule --name <rule name> --at <index>
```

```
Change priority of network packet rule by rule number
```

```
kesl-control [-F] --move-rule --index <index> --at <index>
```

Where:

`--name <rule name>` is the name of the network packet rule.

`--index <index>` is the current number of the rule in the list of network packet rules.

`--at <index>` is the new number of the rule in the list of network packet rules.

kesl-control --add-zone

This command adds an address to a network zone.

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

Where:

`--zone <zone>` is the predefined name of the network zone.

`--address <address>` is the network address or subnet.

kesl-control --del-zone

This command removes an address from a network zone.

```
Remove address from network zone by address or subnet
```

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

```
Remove address from network zone by rule number
```

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

Where:

`--zone <zone>` is the predefined name of the network zone.

`--address <address>` is the network address or subnet.

`--index <address index>` is the number of the address in the network zone.

kesl-control -F --query

This command displays firewall rules created with Kaspersky Endpoint Security.

```
kesl-control -F --query
```

Protection against advanced threats and targeted attacks

Commands for managing the Quarantine

The -Q prefix indicates that the command belongs to the group of commands used to manage the Quarantine.

kesl-control -Q --mass-remove

The command deletes some or all files from Quarantine.

```
Delete all files
kesl-control -Q --mass-remove
```

```
Delete files that match the filter conditions
kesl-control -Q --mass-remove --query "<filter conditions>"
```

Where:

`<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operator> '<value>'` format combined using the logical operator `and` to restrict the results of the query.

kesl-control --put

> This command is available only when Kaspersky Endpoint Security is integrated with Kaspersky Endpoint Detection and Response Optimum or with Kaspersky Managed Detection and Response.

The command allows to quarantine a file.

```
kesl-control [-Q] --put <file path> [--md5] [--sha256] [--save-original-file]
```

Where:

`<file path>` is the path to the file that you want to quarantine.

`--md5` is the MD5 hash of the file that you want to quarantine.

`--sha256` is the SHA256 hash of the file that you want to quarantine.

`--save-original-file` keeps the original file. If you do not specify this option, the original file is deleted.

kesl-control -Q --query

This command outputs information about quarantined files.

```
Output information about all quarantined files
kesl-control -Q --query [-n <number>] [--json]
```

```
Display information about quarantined files that match filter conditions
kesl-control -Q --query ["<filter conditions>"] [-n <number>]
```

Where:

`<filter conditions>` specifies one or more logical expressions in the `<field> <comparison operator> '<value>'` format combined using the logical operator `and` to restrict the results of the query. If you do not specify any filter conditions, the application will display the details of all quarantined files.

`<number>` is the count of the most recent quarantined files that you want to display. If you do not specify the `-n` option, the last 30 files are displayed. To display all files, specify 0.

`--json`: output data in JSON format.

kesl-control -Q --restore

The command lets you restore a file from quarantine.

```
kesl-control -Q --restore <file ID> [--file <file path>]
```

Where:

`<file ID>` is the ID of the quarantined file.

`--file <file path>` is the new name of the file and the path to the directory to save it to. If you do not specify the `--file` option, the file will be restored with its original name and to its original location. If the directory is deleted or the user does not have access rights to it, the application places the file in the /var/opt/kaspersky/kesl/common/restored/ directory. You can manually move the file from this directory to the directory of your choice.

Commands for managing the EDR Expert (on-premises) component

The -R prefix indicates that the command belongs to the group of commands for managing integration settings with Kaspersky Detection and Response solutions.

kesl-control --add-kataedr-server-certificate

This command lets you add or replace a previously added certificate of the KATA server, OSMP threat response server, or OSMP telemetry server (depending on the integration mode).

```
kesl-control [-R] --add-kataedr-server-certificate <file> [--server-type <response|telemetry>]
```

Where:

`<file>` is the path to the file containing the server certificate.

`--server-type <response|telemetry>` lets you select the type of server for which you want to add or replace a certificate in EDR Expert (on-premises) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

If you are adding or replacing a KATA server certificate, omit the `--server-type` option.

kesl-control --remove-kataedr-server-certificate

This command lets you remove a previously added certificate of the KATA server, OSMP threat response server, or OSMP telemetry server (depending on the integration mode).

```
kesl-control [-R] --remove-kataedr-server-certificate [--server-type <response|telemetry>]
```

Where:

`--server-type <response|telemetry>` lets you select the type of server for which you want to remove a certificate in EDR Expert (on-premises) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

If you are removing a KATA server certificate, omit the `--server-type` option.

kesl-control --query-kataedr-server-certificate

This command lets you view information for a previously added certificate of the KATA server, OSMP threat response server, or OSMP telemetry server (depending on the integration mode).

```
kesl-control [-R] --query-kataedr-server-certificate [--server-type <response|telemetry>]
```

Where:

`--server-type <response|telemetry>` lets you select the type of server for which you want to view certificate information in EDR Expert (on-premises) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

If you want to view information about a KATA server certificate, omit the `--server-type` option.

kesl-control --add-kataedr-client-certificate

This command lets you add or replace a previously added client certificate used for protecting the connection to the KATA server, OSMP threat response server, or OSMP telemetry server (depending on the integration mode).

```
kesl-control [-R] --add-kataedr-client-certificate <file>  [--server-type <response|telemetry>]
```

Where:

`<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

> You must specify the password for the crypto container. Otherwise, when you click **Enter**, a `Certificate password is required and cannot be empty` error is displayed.

`--server-type <response|telemetry>` lets you select the type of server for which you want to add a client certificate in EDR Expert (on-premises) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

If you are adding or replacing a client certificate for the connection to a KATA server, omit the `--server-type` option.

kesl-control --remove-kataedr-client-certificate

This command lets you remove a previously added client certificate used for protecting the connection to the KATA server, OSMP threat response server, or OSMP telemetry server (depending on the integration mode).

```
kesl-control [-R] --remove-kataedr-client-certificate [--server-type <response|telemetry>]
```

Where:

`--server-type <response|telemetry>` lets you select the type of server for which you want to remove a client certificate in EDR Expert (on-premises) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

If you are removing a client certificate for the connection to a KATA server, omit the `--server-type` option.

kesl-control --query-kataedr-client-certificate

This command lets you view information about a previously added client certificate used for protecting the connection to the KATA server, OSMP threat response server, or OSMP telemetry server (depending on the integration mode).

```
kesl-control [-R] --query-kataedr-client-certificate [--server-type <response|telemetry>]
```

Where:

`--server-type <response|telemetry>` lets you select the type of server for which you want to view information about a client certificate in EDR Expert (on-premises) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

If you want to view information about a client certificate for the connection to a KATA server, omit the `--server-type` option.

Commands for managing the EDR Expert (cloud) component

The -R prefix indicates that the command belongs to the group of commands for managing integration settings with Kaspersky Detection and Response solutions.

kesl-control --query-cloudxdr-server-certificate

This command lets you view information for a certificate of the OSMP threat response server or OSMP telemetry collection server.

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type <response|telemetry>
```

Where:

`--server-type <response|telemetry>` lets you select the type of server for which you want to view certificate information in EDR Expert (cloud) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

kesl-control --query-cloudxdr-client-certificate

This command lets you view information about a previously added client certificate used for protecting the connection to the OSMP threat response server or OSMP telemetry server.

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type <response|telemetry>
```

Where:

`--server-type <response|telemetry>` lets you select the type of server for which you want to view information about a client certificate in EDR Expert (cloud) integration mode:

- `response` – OSMP threat response action server
- `telemetry` –OSMP telemetry server

Commands for managing the NDR (KATA) component

The -R prefix indicates that the command belongs to the group of commands for managing integration settings with Kaspersky Detection and Response solutions.

kesl-control --add-katandr-server-certificate

This command adds or replaces a previously added NDR server certificate.

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

Where:

`<file>` is the path to the file containing the server certificate.

kesl-control --remove-katandr-server-certificate

This command removes an NDR server certificate.

```
kesl-control [-R] --remove-katandr-server-certificate
```

kesl-control --query-katandr-server-certificate

This command outputs information about an NDR server certificate.

```
kesl-control [-R] --query-katandr-server-certificate
```

kesl-control --add-katandr-client-certificate

This command adds or replaces a previously added client certificate used to secure the connection to an NDR server.

```
kesl-control [-R] --add-katandr-client-certificate <file>
```

Where:

`<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

> You must specify the password for the crypto container. Otherwise, when you click **`Enter`**, a `Certificate password is required and cannot be empty` error is displayed.

kesl-control --remove-katandr-client-certificate

This command deletes the client certificate used to secure the connection to an NDR server.

```
kesl-control [-R] --remove-katandr-client-certificate
```

kesl-control --query-katandr-client-certificate

The command outputs information about a client certificate.

```
kesl-control [-R] --query-katandr-client-certificate
```

Commands for managing device network isolation

The -R prefix indicates that the command belongs to the group of commands for managing integration settings with Kaspersky Detection and Response solutions. Network isolation of devices is applied as a threat response action on threat detection when integrated with the specified Detection and Response solutions.

kesl-control --isolation-stat

This command outputs the current state of network isolation to the console: enabled or disabled.

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

This command lets you disable network isolation of a device.

```
kesl-control [-R] --isolation-off
```

Commands for managing the KUMA integration settings

The -M prefix indicates that the command belongs to the group of commands for managing Kaspersky Unified Monitoring and Analysis Platform settings.

kesl-control --add-kuma-server-certificate

This command adds or replaces a previously added KUMA server certificate.

```
kesl-control [-M] --add-kuma-server-certificate <path to file>
```

Where:

`<path to file>` is the path to the file that contains the server certificate, in DER or PEM format.

kesl-control --remove-kuma-server-certificate

This command removes a KUMA server certificate.

```
kesl-control [-M] --remove-kuma-server-certificate
```

kesl-control --query-kuma-server-certificate

This command outputs information about a KUMA server certificate.

```
kesl-control [-M] --query-kuma-server-certificate
```

kesl-control --add-kuma-client-certificate

This command adds or replaces a previously added client certificate used to secure the connection to a KUMA server.

```
kesl-control [-M] --add-kuma-client-certificate <path to file>
```

Where:

`<path to file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

> You must specify the password for the crypto container. Otherwise, when you click **`Enter`**, a `Certificate password is required and cannot be empty` error is displayed.

kesl-control --remove-kuma-client-certificate

This command deletes the client certificate used to secure the connection to a KUMA server.

```
kesl-control [-M] --remove-kuma-client-certificate
```

kesl-control --query-kuma-client-certificate

The command outputs information about a client certificate.

```
kesl-control [-M] --query-kuma-client-certificate
```

Commands for managing the Sandbox integration settings

The -X prefix indicates that the command belongs to the group of commands for managing the Sandbox integration settings.

kesl-control --add-sandbox-server-certificate

This command adds or replaces a previously added certificate of the server responsible for interaction with Sandbox.

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

Where:

`<file>` is the path to the file that contains the server certificate, in DER or PEM format.

kesl-control --remove-sandbox-server-certificate

This command removes the certificate of the server responsible for interaction with Sandbox.

```
kesl-control [-X] --remove-sandbox-server-certificate
```

kesl-control --query-sandbox-server-certificate

This command displays information about the certificate of the server responsible for interaction with Sandbox.

```
kesl-control [-X] --query-sandbox-server-certificate
```

kesl-control --add-sandbox-client-certificate

This command adds or replaces a previously added client certificate used to secure the connection to the server responsible for interaction with Sandbox.

```
kesl-control [-X] --add-sandbox-client-certificate <file>
```

Where:

`<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

> You must specify the password for the crypto container. Otherwise, when you click **`Enter`**, a `Certificate password is required and cannot be empty` error is displayed.

kesl-control --remove-sandbox-client-certificate

This command removes a client certificate used to secure the connection to the server responsible for interaction with Sandbox.

```
kesl-control [-X] --remove-sandbox-client-certificate
```

kesl-control --query-sandbox-client-certificate

The command outputs information about a client certificate.

```
kesl-control [-X] --query-sandbox-client-certificate
```

kesl-control --sandbox

This command sends files for scanning to Sandbox.

```
kesl-control [-X] --sandbox <path 1> <path 2>
```

Where:

`<path>` is the path to the file or directory that you want to scan. You can specify multiple paths by separating them with a space.

Commands for managing IOC scans

The `-T` prefix indicates that the command belongs to the group of commands for managing application settings and tasks.

kesl-control --scan-ioc

The command starts a search for indicators of compromise on a device (IOC).

```
kesl-control [-T] --scan-ioc --path <path to directory or file> [--process on|off] [--hint <regular expression>]
[--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives all|system|critical|custom] [--
excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

Where:

`--path <path to directory or file>` is the path to IOC file or directory with IOC files with the .IOC or .XML extension, which should be used to perform the scan.

> You can specify multiple paths by separating them with a space. You can also specify both types of paths (path to a file and path to a directory).

`--process` – enable analysis of processes running on the device.

Possible arguments:

- `on` – enable analysis of processes running on the device (default value).
- `off` – disable analysis of processes running on the device.

If you do not specify the `--process` option, the application analyzes processes only if the used IOC file specifies the details of these processes (`ProcessItem`).

`--hint <regular expression>` is the regular expression that matches the full path to the file (`FileItem`) or executable file of the process (`ProcessItem`) to be analyzed.

You can use the following regular expression elements:

- meta characters: `.` `^` `$` `|`
- character classes: `digit`, `alpha`, `lower`, `upper`, `cntrl`
- quantifiers: `*` `+` `?` `{n}` `{n,}` `{n, m}`
- negation: `[^a-c]`
- escaped characters: `\a` `\e` `\f`, `\n` `\r` `\t` `\v` `\b`

`--arpentry` – enable analysis of entries in the ARP table (`ArpEntryItem`).

Possible arguments:

- `on` – enable analysis of entries in the ARP table (default value).
- `off` – disable analysis of entries in the ARP table.

If you do not specify the `--arpentry` option, the application analyzes the ARP table only if the used IOC file specifies the details of the ARP table (`ArpEntryItem`).

`--ports` – enable analysis of ports open for connection.

Possible arguments:

- `on` – enable analysis of ports open for connection and scan active connections on the device (default value).
- `off` – disable analysis of ports open for connection and do not scan active connections on the device.

If you do not specify the `--ports` option, the application only analyzes ports if the used IOC file specifies the details of these ports (`PortItem`).

`--system` – enable analysis of the system environment.

Possible arguments:

- `on` – enable analysis of the system environment (default value).
- `off` – disable analysis of the system environment.

If you do not specify the `--system` option, the application analyzes the system environment only if the used IOC file specifies details of the system environment (`SystemInfoItem`).

`--files` – enable file analysis.

Possible arguments:

- `on` – enable file analysis (default value).
- `off` – disable file analysis.

If you do not specify the `--files` option, the application analyzes files only if the used IOC file specifies the details of those files (`FileItem`).

`--drives` – areas to be scanned.

Possible arguments:

- `all` – check all available file areas.
- `system` – scan all files within the root file system.
- `critical` – scan files in user and system directories (default value).
- `custom` – scan only files in the areas you specify.

If you do not specify the `--drives` option, the application analyzes files in user and system directories.

`--excludes <list of exclusions>` is the list of paths excluded from scanning.

The exclusions specified by this option are global and are valid regardless of the scope type or directory list. These exclusions take precedence over other command line options, including `--hint` and `--scope`.

> Exclusions are specified as paths, but cannot contain recursive elements or wildcard characters (e.g. `*`).

If you do not specify the `--excludes` option, the scan is performed without exclusions.

You can specify multiple exclusions by separating them with a space.

`--scope <list of directories>` is the list of additional directories to be scanned.

> This option is required if you specified the `--drives` argument for the `custom` option.

`--action` – action performed when indicators of compromise are detected.

Possible arguments:

- `Skip` – the application will not perform any actions with the detected object, but information about it will be saved in the task execution results (default value).
- `QuarantineFile` – the application will quarantine the detected object.
- `IsolateHost` – the application imposes network isolation on the device on which the object is detected.
- `ScanCriticalAreas` – the application will perform a Critical Areas Scan.

Critical areas scanned by Kaspersky Endpoint Security

- /lib/systemd
- /lib/udev
- /lib/dbus-1.0
- /usr/local/lib/systemd/user
- /usr/share/dbus-1
- /usr/share/gdm/autostart
- /usr/share/gnome/autostart
- /var/spool/at
- /var/spool/at/spool
- /var/spool/anacron

- /var/spool/cron
- /boot
- /bin
- /sbin
- /lib
- /lib32
- /lib64
- /libx32
- /usr/lib
- /usr/lib32
- /usr/lib64
- /usr/libx32
- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

You can specify multiple actions by separating them with commas.

> If you specify the `Skip` argument, do not add any other arguments. The `Skip` argument can only be used on its own.

kesl-control --get-response-task-list

This command displays information about running *IOC Scan* tasks on the device.

```
kesl-control [-T] --get-response-task-list
```

As a result, the application displays information about running tasks in the following form:

Task ID: <task ID>

Response action: locScan

Creation date: <date and time of task creation>

Start task: <task launch schedule>

State: <task status>

Kaspersky Endpoint Security updates information about running *IOC Scan* tasks at each synchronization with the server. You can configure the synchronization period in the settings of the integration with the Kaspersky Detection and Response solution (`SynchronizationPeriod`). By default, the application synchronizes with the server every 5 minutes.

kesl-control --delete-response-task <task ID>

This command deletes the *IOC Scan* task by ID. The application deletes the task locally on the computer. If you have not deleted the task in the Web Console or OSMP Console, the application restores this task the next time it is synchronized with the server.

```
kesl-control [-T] --delete-response-task-list <task ID>
```

Application commands in Light Agent mode

The -V prefix indicates that the command belongs to the group of commands of Kaspersky Endpoint Security used in Light Agent mode.

> The commands can be executed only if Kaspersky Endpoint Security is used in Light Agent mode.

kesl-control --ksvla-info

This command outputs information about using the application in Light Agent mode.

```
kesl-control --ksvla-info
```

kesl-control --viis-info

This command outputs information about connecting the application in Light Agent mode to the Integration Server.

```
kesl-control --viis-info
```

kesl-control --svm-info

This command outputs information about connecting the application in Light Agent mode to the SVM.

```
kesl-control --svm-info
```

Application command-line options

Update task

The following table describes all available values and default values of all the settings that you can specify for the `Update` task.

Update task settings

Setting	Description	Values
`ConnectionTimeout`	Response timeout (in seconds) of an update source while attempting to connect to it. If an update source does not respond within the specified time interval, the application contacts the next update source in the list.	You can use only integers within the range from 0 to 120. Default value: 10.
`ApplicationUpdateMode`	How automatically installed application updates (autopatches) are downloaded and installed.	`Disabled`: do not download or install autopatches. `DownloadOnly` (default): download autopatches, but do not install them. `DownloadAndInstall`: automatically download and install autopatches. After an autopatch is installed, the application restarts automatically.
The **[Sources.item_#]** section contains the following settings:		
`Enabled`	Use of the update source specified in the `SourceType` setting. To run the task, at least one update source needs to be enabled.	`Yes` (default) – the application is using the update source. `No` – the application is not using the update source.

Setting	Description	Values
`SourceType`	Source from which the application receives updates.	`KLServers` (default value) — The application receives updates from one of the Kaspersky update servers. Updates are downloaded via HTTPS protocol. `SCServer`. The application downloads updates to the protected device from the Administration Server installed on the local network. You can select this update source if you use Kaspersky Security Center for centralized administration of device protection in your organization. `Custom`. The application downloads updates from a custom source specified in the `URL` setting. You can specify directories on FTP, HTTP, and HTTPS servers or directories on any device mounted on the protected client device, including directories on remote devices mounted via the Samba or NFS protocols.
`URL`	Address of the custom update source on the local area network or the Internet.	The default value is not defined. Examples: `URL=http://example.com/bases/` – address of the HTTP server with the directory that contains updates. `URL=/home/bases/` – directory on the protected computer that contains application databases.

Host Threat Protection

File Threat Protection task

In the command line, you can manage File Threat Protection using the File Threat Protection predefined task (`File_Threat_Protection`).

The File Threat Protection task is started by default. You can start and stop this task manually.

> Administrator role privileges are required to start and stop the File Threat Protection task from the command line.

You can configure File Threat Protection settings by editing the settings of the File Threat Protection predefined task.

The following table describes all possible values and default values of all settings that you can specify for the File Threat Protection task.

Setting	Description	Values
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used. We do not recommend enabling this setting because scanning archives impacts performance due to the fact that access to the archive file is blocked while the file is being unpacked to a temporary directory and scanned.	`Yes` —Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` (default value) — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` — Scan self-extracting archives. `No` (default value) — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`SkipPlainTextFiles`	Temporary exclusion of files in text format from scans. This setting makes it possible to optimize scans of application logs. This setting is applied if you use system event interception mechanism based on fanotify. When using an updatable kernel module, the scan is optimized by using the scan result cache.	`Yes` – Do not scan text files if they are reused by the same process for 10 minutes after the most recent scan. `No` (default value) – scan files in plain text format.
`SkipDatabaseJournals`	Temporarily excluding database journal files from scanning. This setting makes it possible to optimize scans of database journal files. This setting is applied if you use system event interception mechanism based on fanotify. When using an updatable kernel module, the scan is optimized by using the scan result cache.	`Yes` – Do not scan database journal files if they are reused by the same process within 10 minutes after the most recent scan. `No` (default) – Scan database journal files.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 60.

Setting	Description	Values
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectBlockIfNotPossible` (disinfect; block if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application blocks access to the infected object. `Block` – The application blocks access to an infected object. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the scan.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask.
	You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.
		The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Enables exclusion of objects containing the threats specified by the `ExcludeThreats.item_#` setting from scans.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		Example
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) — Do not log information about non-infected objects.
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) — Do not log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) — Do not log information about unprocessed objects.

Setting	Description	Values
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts. This setting is not applicable to devices with an Elbrus CPU.	`Yes` (default value) — Enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning. This setting is not applicable to devices with an Elbrus CPU.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) — The recommended value.
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) — Enable use of the iChecker technology. `No` — Disable use of the iChecker technology.
`ScanByAccessType`	File Threat Protection task operation mode. The `ScanByAccessType` setting only applies to the File Threat Protection task.	`SmartCheck` (default value) — Scan a file on attempts to open it, and scan it again on attempts to close it if the file has been modified. If a process accesses an object multiple times in the course of its operation and modifies it, the application scans the object again only when the process closes it for the last time. `OpenAndModify` — Scan a file on attempts to open it, and scan it again on attempts to close it if the file has been modified. `Open` — Scan a file on attempts to open it for reading, execution, or modification.
The **[ScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan scope, which contains additional information about the scan scope. The maximum length of the string specified using this setting is 4096 characters.	Default value: `All objects`. Example `AreaDesc="Scanning of email databases"`
`UseScanArea`	Enables scans of the specified scope. To run the task, enable scans of at least one scope.	`Yes` (default value) — Scan the specified scope. `No` — Do not scan the specified scope.
`AreaMask.item_#`	Scan scope limitation. With this scan scope, the application only scans files that are specified using masks in the shell format. If this setting is not specified, the application scans all the objects in the scan scope. You can specify several values for this setting.	The default value is `*` (scan all objects). Example `AreaMask_item_<item number>=*doc`

Setting	Description	Values
`Path`	Path to the directory with objects to be scanned.	`<path to local folder>` – Scan objects in the specified directory. You can use masks and tags to specify the path. `Shared:NFS` — Scan the device file system resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samba protocol. `Mounted:NFS` – Scan the remote directories mounted on a device using the NFS protocol. `Mounted:SMB` – Scan the remote directories mounted on a device using the Samba protocol. `AllRemoteMounted` – Scan all remote directories mounted on the device using the Samba and NFS protocols. `AllShared` – Scan all the device file system resources that are accessible via the Samba and NFS protocols. `<file system type>` – Scan all resources of the specified file system device.
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan exclusion scope, which contains additional information about the exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.
`AreaMask.item_#`	Limitation of scan exclusion scope. In the exclusion scope, the application excludes from scans only files that are specified using masks in the shell format. If this setting is not specified, the application does not scan any of the objects within the exclusion scope. You can specify several values for this setting.	Default value: `*` (exclude all objects from scan)
`Path`	Path to the directory with objects to be excluded.	`<path to local folder>` – Exclude objects in the specified directory (including subdirectories) from scans. You can use masks and tags to specify the path. `Mounted:NFS` – Exclude the remote directories mounted on a device using the NFS protocol from scan. `Mounted:SMB` – Exclude the remote directories mounted on a device using the Samba protocol from scan. `AllRemoteMounted` – Exclude all remote directories mounted on the device using the Samba and NFS protocols from scan. `<file system>` – Exclude from scanning all resources of the specified file system device.
The **[ExcludedForProgram.item_#]** section contains the following settings:		
`ProgramPath`	Path to excluded process. If the updatable kernel module is used for system event interception, the specified process is excluded from interception in all namespaces.	`<path to process>` — Exclude objects in the specified directory from scanning.
`ApplyToDescendants`	Exclude child processes of the excluded process specified by the `ProgramPath` setting from scans.	`Yes` – exclude the specified process and all its child processes from scans. `No` (default value) – exclude only the specified process from scans, do not exclude its child processes from scans.
`AreaDesc`	Description of the process exclusion scope.	Default value: `All objects`.
`UseExcludedForProgram`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.

Setting	Description	Values
`AreaMask.item_#`	Limitation of the process exclusion scope. In the process exclusion scope, the application excludes from scans only the files that are specified using masks in the shell format. If this setting is not specified, the application excludes from scans all the objects within the process exclusion scope. You can specify several values for this setting.	Default value: `*` (exclude all objects from scan)
`Path`	Path to a directory with files that are modified by the process.	`<path to local folder>` — Exclude objects in the specified directory from scanning. You can use masks to specify the path. `Shared:NFS` — Exclude device file system resources that are accessible via the NFS protocol from scans. `Shared:SMB` — Exclude device file system resources that are accessible via the Samba protocol from scans. `Mounted:NFS` – Exclude the remote directories mounted on a device using the NFS protocol from scan. `Mounted:SMB` – Exclude the remote directories mounted on a device using the Samba protocol from scan. `AllRemoteMounted` – Exclude all remote directories mounted on the device using the Samba and NFS protocols from scan. `AllShared` – Exclude all device file system resources that are accessible using the Samba and NFS protocols from scan. `<file system type>` – Exclude from scanning all resources of the specified file system device.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Optimizing network directory scanning

To optimize the File Threat Protection task, you can exclude from scans any files being copied from network directories to the local directory. To do so, configure exclusion based on processes for the utility used for copying from network directories (for example, for the `cp` utility).

To configure exclusion of network directories from scans:

1. Output File Threat Protection task settings (`File_Threat_Protection`, ID:1) to a configuration file using the following command:

   ```
   kesl-control --get-settings 1 --file <full path to the configuration file> [--json]
   ```

2. Open the configuration file and add the `[ExcludedForProgram.item_#]` section with the following settings:

   - `ProgramPath` – path to the process to be excluded or to the directory with the processes to be excluded.
   - `ApplyToDescendants` is a parameter that indicates whether the scan should exclude child processes of the excluded process (possible values: `Yes` or `No`).
   - `AreaDesc` – a description of the process exclusion scope, which contains additional information about the exclusion scope.

- `UseExcludedForProgram` enables exclusion of the specified scope during task operation (possible values: `Yes` or `No`).
- `Path` – path to the files or directory with files modified by the process.
- `AreaMask.item_#` is the file name mask for the files to be excluded from the scan. You can also specify the full path to the file.

Example

```
[ExcludedForProgram.item_0000]
ProgramPath=/usr/bin/cp
ApplyToDescendants=No
AreaDesc=
UseExcludedForProgram=Yes
Path=AllRemoteMounted
AreaMask.item_0000=*
```

3. Run the following command:

```
kesl-control --set-settings 1 --file <full path to the configuration file> [--json]
```

Specify the `--json` option if you are importing settings from a configuration file in JSON format. If the option is not specified, the application will attempt to import settings from an INI file. If the import fails, an error is displayed.

The application does not scan the files in network directories, but the `cp` command itself (for the example given above) and local files are scanned.

Malware Scan

On the command line, you can scan for malware in the following ways:

- Using the Malware Scan predefined task (`Scan_My_Computer`). You can manually start, stop, pause, or resume this task and configure the task schedule. You can configure scan settings by editing the settings of this task.
- Using Malware Scan custom tasks (tasks of the `ODS` type). You can manually start, stop, pause, or resume user tasks and configure the task schedule.

You can perform a *custom scan* of specified files and directories using the following command:

```
kesl-control --scan-file
```

Malware Scan task

The table describes all possible values and the default values of all the settings that you can specify for the Malware Scan task (`Scan_My_Computer`).

Setting	Description	Values
`ScanFiles`	Enables file scan.	`Yes` (default value) — Scan files. `No` — Do not scan files.
`ScanBootSectors`	Enables boot sector scans.	`Yes` (default value) — Scan boot sectors. `No` — Do not scan boot sectors.
`ScanComputerMemory`	Enables process memory and kernel memory scans.	`Yes` (default value) — Scan process memory and kernel memory. `No` — Do not scan process memory and kernel memory.
`ScanStartupObjects`	Enables startup object scans.	`Yes` (default value) — Scan startup objects. `No` — Do not scan startup objects.
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used.	`Yes` (default value) — Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` (default value) — Scan self-extracting archives. `No` — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 0.
`QueueScanTasks`	Delay scheduled scan tasks if a previously started scheduled scan is still running. Kaspersky Endpoint Security will enqueue scheduled scan tasks if the current scan continues. This helps optimize the load on the computer. For example, a scan task is scheduled to run at 6:00 PM and at 8:00 PM. The scan task that is scheduled to run at 8:00 PM is delayed if the 6:00 PM scan is still running. The delayed task is run after the 6:00 PM task finishes.	`Yes` to enqueue scheduled scan tasks if the current scan is still running. `No` (default value) to run scheduled scan tasks even if the current scan is still running.

Setting	Description	Values
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectInformIfNotPossible` (disinfect; inform if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. `Inform` means the application does not try to disinfect or delete the infected object. Information about the infected object is logged. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the scan.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.
	Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled.
		The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Enables exclusion of objects containing the threats specified by the `ExcludeThreats.item_#` setting from scans.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		Example
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Enables global exclusions for scanning.	`Yes` (default value) — Use the global exclusions. `No` — Do not use global exclusions.
`UseOASExclusions`	Enables File Threat Protection exclusions for scanning.	`Yes` (default value) — Use File Threat Protection exclusions. `No` — do not use File Threat Protection exclusions.
`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) — Do not log information about non-infected objects.

Setting	Description	Values
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) — Do not log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) — Do not log information about unprocessed objects.
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts.	`Yes` (default value) — Enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. You can specify the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) — The recommended value.
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) — Enable use of the iChecker technology. `No` — Disable use of the iChecker technology.
`DeviceNameMasks.item_#`	List of device names. The application will scan boot sectors of these devices. The setting value cannot be empty. At least one device name mask must be specified to run this task.	`AllObjects` – scan boot sectors of all devices. `<device name mask>` – Scan boot sectors of the devices whose names match the specified mask. Default value: `/**` – any set of characters in the device name, including the `/` character.
The **[ScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan scope, which contains additional information about the scan scope. The maximum length of the string specified using this setting is 4096 characters.	Default value: `All objects`. Example `AreaDesc="Mail bases scan"`
`UseScanArea`	Enables scans of the specified scope. To run the task, enable scans of at least one scope.	`Yes` (default value) — Scan the specified scope. `No` — Do not scan the specified scope.
`AreaMask.item_#`	Scan scope limitation. Within the scan scope, the application scans only the files that are specified using the masks in the shell format. If this setting is not specified, the application scans all the objects in the scan scope. You can specify several values for this setting.	The default value is `*` (scan all objects). Example `AreaMask.item_0000=*doc`

Setting	Description	Values
`Path`	Path to the directory with objects to be scanned.	`<path to local directory>` – Scan objects in the specified directory. `Shared:NFS` — Scan the device file system resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samba protocol. `Mounted:NFS` – Scan the remote directories mounted on a device using the NFS protocol. `Mounted:SMB` – Scan the remote directories mounted on a device using the Samba protocol. `AllRemoteMounted` – Scan all remote directories mounted on the device using the Samba and NFS protocols. `AllShared` – Scan all the device file system resources that are accessible via the Samba and NFS protocols. `<file system type>` – Scan all resources of the specified file system device.
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan exclusion scope, which contains additional information about the exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.
`AreaMask.item_#`	Limitation of scan exclusion scope. In the exclusion scope, the application excludes only the files that are specified using masks in the shell format. If this setting is not specified, the application excludes all the objects in the exclusion scope. You can specify several values for this setting.	Default value: `*` (exclude all objects)
`Path`	Path to the directory with objects to be excluded.	`<path to local directory>` – Exclude objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path. In order to optimize the operation of scan tasks, it is recommended to add the path with snapshots mounted by the system in the read-only mode to the exclusions for the systems with the btrfs file system and enabled active snapshots. For example, for the systems based on SUSE/OpenSUSE, you can add the following exclusion `/.snapshots/*/snapshot/`. The `/` path is specified by default. The application excludes all directories of the local file system from scan. `Mounted:NFS` – Exclude the remote directories mounted on a device using the NFS protocol from scan. `Mounted:SMB` – Exclude the remote directories mounted on a device using the Samba protocol from scan. `AllRemoteMounted` – Exclude all remote directories mounted on the device using the Samba and NFS protocols from scan. `<file system type>` – Exclude from scanning all resources of the specified file system device. Remote directories are excluded from scanning by the application only if they were mounted before the task was started. Remote directories mounted after the task is started are not excluded from scanning.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Custom Scan task

The table describes all available values and the default values of all the settings that you can specify for the Custom Scan task (`Scan_File`).

Custom Scan task settings

Setting	Description	Values
`ScanFiles`	Enables file scan.	`Yes` (default value) — Scan files. `No` — Do not scan files.
`ScanBootSectors`	Enables boot sector scans.	`Yes` — Scan boot sectors. `No` (default value) — Do not scan boot sectors.
`ScanComputerMemory`	Enables process memory and kernel memory scans.	`Yes` — Scan process memory and kernel memory. `No` (default value) — Do not scan process memory and kernel memory.
`ScanStartupObjects`	Enables startup object scans.	`Yes` — Scan startup objects. `No` (default value) — Do not scan startup objects.
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used.	`Yes` (default value) — Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` (default value) — Scan self-extracting archives. `No` — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.

Setting	Description	Values
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 0.
`QueueScanTasks`	Delay scheduled scan tasks if a previously started scheduled scan is still running. Kaspersky Endpoint Security will enqueue scheduled scan tasks if the current scan continues. This helps optimize the load on the computer. For example, a scan task is scheduled to run at 6:00 PM and at 8:00 PM. The scan task that is scheduled to run at 8:00 PM is delayed if the 6:00 PM scan is still running. The delayed task is run after the 6:00 PM task finishes.	`Yes` to enqueue scheduled scan tasks if the current scan is still running. `No` (default value) to run scheduled scan tasks even if the current scan is still running.
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectInformIfNotPossible` (disinfect; inform if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. `Inform` means the application does not try to disinfect or delete the infected object. Information about the infected object is logged. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the scan.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) not to exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.	The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Enables exclusion of objects containing the threats specified by the `ExcludeThreats.item_#` setting from scans.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		Example
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Enables global exclusions for scanning.	`Yes` (default value) to use the global exclusions. `No` — Do not use global exclusions.

Setting	Description	Values
`UseOASExclusions`	Enables File Threat Protection exclusions for scanning.	`Yes` (default value) to use File Threat Protection exclusions. `No` — do not use File Threat Protection exclusions.
`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) not to log information about non-infected objects.
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) not to log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) not to log information about unprocessed objects.
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts.	`Yes` (default value) to enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. You can specify the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) – The recommended value.
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) to enable use of the iChecker technology. `No` — Disable use of the iChecker technology.
`DeviceNameMasks.item_#`	List of device names. The application will scan boot sectors of these devices. The setting value cannot be empty. At least one device name mask must be specified to run this task.	`AllObjects` – scan boot sectors of all devices. `<device name mask>` – Scan boot sectors of the devices whose names match the specified mask. Default value: `/**` – any set of characters in the device name, including the `/` character.

Critical Areas Scan task

The table below describes all available values and the default values of all the settings that you can specify for the Critical Areas Scan task (`Critical_Areas_Scan`).

Critical Areas Scan task settings

Setting	Description	Values
`ScanFiles`	Enables file scan.	`Yes` — Scan files. `No` (default value) — Do not scan files.
`ScanBootSectors`	Enables boot sector scans.	`Yes` (default value) — Scan boot sectors. `No` — Do not scan boot sectors.
`ScanComputerMemory`	Enables process memory and kernel memory scans.	`Yes` (default value) — Scan process memory and kernel memory. `No` — Do not scan process memory and kernel memory.
`ScanStartupObjects`	Enables startup object scans.	`Yes` (default value) — Scan startup objects. `No` — Do not scan startup objects.

Setting	Description	Values
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used.	`Yes` (default value) — Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` (default value) — Scan self-extracting archives. `No` — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 0.
`QueueScanTasks`	Delay scheduled scan tasks if a previously started scheduled scan is still running. Kaspersky Endpoint Security will enqueue scheduled scan tasks if the current scan continues. This helps optimize the load on the computer. For example, a scan task is scheduled to run at 6:00 PM and at 8:00 PM. The scan task that is scheduled to run at 8:00 PM is delayed if the 6:00 PM scan is still running. The delayed task is run after the 6:00 PM task finishes.	`Yes` to enqueue scheduled scan tasks if the current scan is still running. `No` (default value) to run scheduled scan tasks even if the current scan is still running.
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectInformIfNotPossible` (disinfect; inform if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. `Inform` means the application does not try to disinfect or delete the infected object. Information about the infected object is logged. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the scan.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.
	Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled.
		The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

Setting	Description	Values
`UseExcludeThreats`	Enables exclusion of objects containing the threats specified by the `ExcludeThreats.item_#` setting from scans.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		`Example`
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Enables global exclusions for scanning.	`Yes` (default value) — Use the global exclusions. `No` — Do not use global exclusions.
`UseOASExclusions`	Enables File Threat Protection exclusions for scanning.	`Yes` (default value) — Use File Threat Protection exclusions. `No` — do not use File Threat Protection exclusions.
`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) — Do not log information about non-infected objects.
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) — Do not log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) — Do not log information about unprocessed objects.
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts.	`Yes` (default value) — Enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. You can specify the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) — The recommended value.
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) — Enable use of the iChecker technology. `No` — Disable use of the iChecker technology.

Setting	Description	Values
`DeviceNameMasks.item_#`	List of device names. The application will scan boot sectors of these devices. The setting value cannot be empty. At least one device name mask must be specified to run this task.	`AllObjects` – scan boot sectors of all devices. `<device name mask>` – Scan boot sectors of the devices whose names match the specified mask. Default value: `/**` – any set of characters in the device name, including the `/` character.
The **[ScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan scope, which contains additional information about the scan scope. The maximum length of the string specified using this setting is 4096 characters.	Default value: `All objects`. Example `AreaDesc="Mail bases scan"`
`UseScanArea`	Enables scans of the specified scope. To run the task, enable scans of at least one scope.	`Yes` (default value) — Scan the specified scope. `No` — Do not scan the specified scope.
`AreaMask.item_#`	Scan scope limitation. Within the scan scope, the application scans only the files that are specified using the masks in the shell format. If this setting is not specified, the application scans all the objects in the scan scope. You can specify several values for this setting.	The default value is `*` (scan all objects). Example `AreaMask.item_0000=*doc`
`Path`	Path to the directory with objects to be scanned.	`<path to local directory>` – Scan objects in the specified directory. `Shared:NFS` — Scan the device file system resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samba protocol. `Mounted:NFS` – Scan the remote directories mounted on a device using the NFS protocol. `Mounted:SMB` – Scan the remote directories mounted on a device using the Samba protocol. `AllRemoteMounted` – Scan all remote directories mounted on the device using the Samba and NFS protocols. `AllShared` – Scan all the device file system resources that are accessible via the Samba and NFS protocols. `<file system type>` – Scan all resources of the specified file system device.
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan exclusion scope, which contains additional information about the exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.
`AreaMask.item_#`	Limitation of scan exclusion scope. In the exclusion scope, the application excludes only the files that are specified using masks in the shell format. If this setting is not specified, the application excludes all the objects in the exclusion scope. You can specify several values for this setting.	Default value: `*` (exclude all objects)

Setting	Description	Values
`Path`	Path to the directory with objects to be excluded.	`<path to local directory>` – Exclude objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path. In order to optimize the operation of scan tasks, it is recommended to add the path with snapshots mounted by the system in the read-only mode to the exclusions for the systems with the btrfs file system and enabled active snapshots. For example, for the systems based on SUSE/OpenSUSE, you can add the following exclusion `/.snapshots/*/snapshot/`. The `/` path is specified by default. The application excludes all directories of the local file system from scan. `Mounted:NFS` – Exclude the remote directories mounted on a device using the NFS protocol from scan. `Mounted:SMB` – Exclude the remote directories mounted on a device using the Samba protocol from scan. `AllRemoteMounted` – Exclude all remote directories mounted on the device using the Samba and NFS protocols from scan. `<file system type>` – Exclude from scanning all resources of the specified file system device. Remote directories are excluded from scanning by the application only if they were mounted before the task was started. Remote directories mounted after the task is started are not excluded from scanning.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Removable drives scan task

In the command line, you can manage the removable drives scan using the Removable Drives Scan predefined task (`Removable_Drives_Scan`).

Removable Drives Scan is not running by default. You can start and stop this task manually. You can configure scan settings by editing the settings of this task.

If the task is running, the application monitors the connection of removable drives to the device and, when a removable drive is connected, it creates and starts a temporary boot sector scan task (task of the `ODS` type). This task cannot be stopped. After the task execution completes, the application automatically deletes the task.

If you enabled file scanning in the *Removable Drives Scan* task settings, the application also starts one or more temporary custom file scan tasks (tasks of the `ODS` type). If necessary, a user with administrator privileges can stop these tasks.

If you modify the *Removable Drives Scan* task settings, the new values are not applied to temporary tasks that are already running. Stopping the *Removable Drives Scan* task does not stop temporary tasks that are already running.

Removable Drives Scan task settings

Setting	Description	Values
`ScanRemovableDrives`	Enables the scanning of removable media when it is connected to the device. This setting does not apply to CD/DVD drives and Blu-ray discs (see the `ScanOpticalDrives` setting).	`DetailedScan`. Scan all files on removable media (except CD/DVD and Blu-ray discs). A detailed scan is performed with the default settings for the `Scan_File` task (ID: 3). `QuickScan`. Scan only files of **specific types** on removable media (except CD/DVD and Blu-ray discs). The following file formats are scanned on removable media: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. A quick scan is performed with the default settings for the `Critical_Areas_Scan` task (ID: 4). `NoScan` (default value) — Do not scan removable media when it is connected to the device.
`ScanOpticalDrives`	Enables the scanning of CD/DVD drives and Blu-ray discs when they are connected to the device.	`DetailedScan`. Scan all files on CD/DVD drives and Blu-ray discs. A detailed scan is performed with the default settings for the `Scan_File` task (ID: 3). `QuickScan`. Scan only files of **specific types** on CD/DVD drives and Blu-ray discs. The following file formats are scanned on removable media: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. A quick scan is performed with the default settings for the `Critical_Areas_Scan` task (ID: 4). `NoScan` (default value). Do not scan CD/DVD drives and Blu-ray discs when they are connected.
`BlockDuringScan`	Enables the blocking of files on a connected disk during scanning. While scanning boot sectors, files are not blocked.	`Yes` — Block files during the scan. `No` (default value) — Do not block files during the scan.

Container Scan

On the command line, you can scan containers and images in the following ways:

- Using the Container Scan predefined task (`Container_Scan`). You can manually start or stop this task, and configure the task schedule. You can configure scan settings by editing the settings of this task.
- Using Container Scan user tasks (tasks of the `ContainerScan` type). You can manually start and stop user tasks and configure the task schedule.

- Using the following command, you can perform a *custom scan* of the specified containers and images:

```
kesl-control --scan-container
```

Container Scan settings

The following table describes container scan settings that are used when scanning namespaces and containers in real time.

General container and namespace scan settings

Setting	Description	Values
`OnAccessContainerScanAction`	Action to be performed on a container when an infected object is detected. This setting is available when using the application under a license that supports this function. File Threat Protection task settings are used when scanning objects inside a container.	`StopContainerIfFailed` (default value) — Stop the container if an infected object cannot be disinfected or deleted. If this value is specified, the action performed on the container also depends on the `ActionOnThreat` setting of the File Threat Protection task. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible` and the application cannot disinfect or delete the infected object while carrying out the action, the container is stopped. `StopContainer` — Stop the container when an infected object is detected. `Skip` — Do not perform any action on containers when an infected object is detected.
`UseDocker`	Using the Docker container management system.	`Yes` (default) enables the use of the Docker container management system. `No` disables the use of the Docker container management system.
`DockerSocket`	Docker socket path or URI (Universal Resource Identifier).	Default value: /var/run/docker.sock.
`UseCrio`	Use the CRI-O environment.	`Yes` (default value) — Use the CRI-O environment. `No` — Do not use the CRI-O environment.
`CrioConfigFilePath`	Path to the CRI-O configuration file.	Default value: /etc/crio/crio.conf.
`UsePodman`	Use the Podman utility.	`Yes` (default value) — Use the Podman utility. `No` — Do not use the Podman utility.
`PodmanBinaryPath`	Path to the Podman utility executable file.	Default value: /usr/bin/podman.
`PodmanRootFolder`	Path to the root directory of the container storage.	Default value: /var/lib/containers/storage.
`UseRunc`	Use the runc utility.	`Yes` (default value) — Use the runc utility. `No`: do not use the runc utility.
`RuncBinaryPath`	Path to the runc utility executable file.	Default value: /usr/bin/runc.
`RuncRootFolder`	Path to the root directory of the container state storage.	Default value: /run/runc.

Container scan task

The table describes all available values and the default values of all the settings you can specify for the Container Scan task (`Container_Scan`).

Container Scan task settings

Setting	Description	Values
`ScanContainers`	Scan of containers specified by mask You can specify masks using the `ContainerNameMask` setting.	`Yes` (default value) — Scan containers defined by mask. `No` — Do not scan containers defined by mask.

`ContainerNameMask`	Specifies a name or a name mask that defines a container to scan.
	Masks are specified in command shell format. You can use the ? and * symbols.
	Before specifying this setting, make sure that `ScanContainers=Yes`.
		Default value: * (scan all containers).
		`Example of a container scan performed on a container named my_container`
		`ContainerNameMask=my_container`
		`Example of scanning all containers whose names start with my_container`
		`ContainerNameMask=my_container*`
		`Example of a container scan performed on all containers whose names start with my_, then contain any five characters, then _container, and end with any characters sequence`
		`ContainerNameMask=my_?????_container*`

`ScanImages`	Scan of images specified by mask You can specify masks using the `ImageNameMask` setting.	`Yes` (default value) — Scan images defined by mask. `No` — Do not scan images defined by mask.

`ImageNameMask`	Specifies a name or a name mask that define images to scan.
	Before specifying this setting, make sure that the `ScanImages` setting is set to `Yes`.
	Masks are specified in command shell format.
	If you want to specify several masks, each mask must be specified on a new line with a new index.
		Default value: * (scan all images).
		`Example of an image scan performed on images with the "my_image" name, and the "latest" tag`
		`ImageNameMask=my_image:latest`
		`Example of an image scan performed on all images whose names start with my_image_ and with any tag`
		`ImageNameMask=my_image*`

`DeepScan`	Checking all image layers and running containers.	`Yes` – Scan all layers. `No` (default value) – Do not scan any layer.
`ContainerScanAction`	Action to be performed on a container when an infected object is detected. Actions on an infected object inside the container are described below.	`StopContainerIfFailed` (default value) — The application stops the container if an infected object could not be disinfected or deleted. If this value is selected, the action performed with the container also depends on the `ActionOnThreat` setting, which is applied to objects inside containers and images (see the table below). If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible` and the application cannot disinfect or delete the infected object while carrying out the action, the container is stopped. Due to the way a CRI-O environment works, an infected object is not disinfected or deleted in a container in a CRI-O environment. We recommend selecting the `StopContainer` action. `StopContainer` — The application stops the container when an infected object is detected. `Skip` — The application does not perform any action on containers when an infected object is detected.

Setting	Description	Values
`ImageAction`	Specifies the action to be performed on an image when an infected object is detected. Actions on an infected object inside the image are described below.	`Skip` (default value) — The application does not perform any action on images when an infected object is detected. `Delete` — The application deletes the image when an infected object is detected (not recommended). All dependencies will also be deleted. Running containers will be stopped, and then deleted.

The settings described below are applied to the objects inside containers and images.

Container Scan task settings

Setting	Description	Values
`ScanArchived`	Enables scanning of archives (including SFX self-extracting archives). The application scans the following archives: .zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj. The list of supported archive formats depends on the application databases being used.	`Yes` (default value) — Scan archives. If `ActionOnThreat` is set to `DisinfectDeleteIfNotPossible`, and disinfection is impossible, then, depending on the archive type, the application deletes either the infected object or the entire archive that contains the threat. `No` — Do not scan archives.
`ScanSfxArchived`	Enables scanning of self-extracting archives only (archives that contain an executable extraction module).	`Yes` (default value) — Scan self-extracting archives. `No` — Do not scan self-extracting archives.
`ScanMailBases`	Enables scanning email databases of Microsoft Outlook, Outlook Express, The Bat, and other mail clients.	`Yes` — Scan files of email databases. `No` (default value) — Do not scan files of email databases.
`ScanPlainMail`	Enables scanning of plain text email messages.	`Yes` — Scan plain text email messages. `No` (default value) — Do not scan plain text email messages.
`TimeLimit`	Maximum object scan duration (in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	0 to 9999 0 — The object scan time is unlimited. Default value: 0.
`SizeLimit`	Maximum size of an object to be scanned (in megabytes). If the object to be scanned is larger than the specified value, the application skips this object.	0 to 999999 0 — The application scans objects of any size. Default value: 0.
`ActionOnThreat`	Selection of the action to be performed by the application on the infected objects.	`DisinfectDeleteIfNotPossible` (disinfect; delete if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. `DisinfectInformIfNotPossible` (disinfect; inform if not possible) means the application tries to disinfect the infected object after saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. `Inform` means the application does not try to disinfect or delete the infected object. Information about the infected object is logged. Default value: `DisinfectDeleteIfNotPossible`.
`UseExcludeMasks`	Uses scan exclusions for the objects specified by the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scans. `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from the scan.

Setting	Description	Values

`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format.	The default value is not defined.
		Example
		`UseExcludeMasks=Yes`
		`ExcludeMasks.item_0000=eicar1.*`
		`ExcludeMasks.item_0001=eicar2.*`

`UseExcludeThreats`	Uses scan exclusions for objects containing the threats specified by the `ExcludeThreats.item_#` setting.	`Yes` — Exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan. `No` (default value): do not exclude objects containing the threats specified by the `ExcludeThreats.item_#` setting from the scan.

`ExcludeThreats.item_#`	Excludes objects from scans by the name of the threats detected in them. Before specifying a value for this setting, make sure that the `UseExcludeThreats` setting is enabled.
	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected.
	For example, you may be using a utility to obtain information about your network. To keep the application from blocking it, add the full name of the threat contained in it to the list of threats excluded from scans.
	You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
		The setting value is case-sensitive.
		The default value is not defined.
		Example
		`UseExcludeThreats=Yes`
		`ExcludeThreats.item_0000=EICAR-Test-*`
		`ExcludeThreats.item_0001=?rojan.Linux`

`UseGlobalExclusions`	Enables global exclusions for scanning.	`Yes` (default value) — Use the global exclusions. `No` — Do not use global exclusions.
`ReportCleanObjects`	Enables logging of information about scanned objects that the application reports as not being infected. You can enable this setting, for example, to make sure that a particular object was scanned by the application.	`Yes` — Log information about non-infected objects. `No` (default value) — Do not log information about non-infected objects.
`ReportPackedObjects`	Enables logging of information about scanned objects that are part of compound objects. You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`Yes` — Log information about scanned objects within archives. `No` (default value) — Do not log information about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocessed objects. `No` (default value) — Do not log information about unprocessed objects.
`UseAnalyzer`	Enables heuristic analysis. Heuristic analysis helps the application to detect threats even before they become known to virus analysts.	`Yes` (default value) — Enable Heuristic Analyzer. `No` — Disable Heuristic Analyzer.
`HeuristicLevel`	Specifies the heuristic analysis level. You can specify the heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for threats, the load on the operating system's resources, and the scan duration. The higher the heuristic analysis level, the more resources and time are required for scanning.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis level with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system. `Recommended` (default value) — The recommended value.

Setting	Description	Values
`UseIChecker`	Enables usage of the iChecker technology.	`Yes` (default value) — Enable use of the iChecker technology. `No` — Disable use of the iChecker technology.
`QueueScanTasks`	Delay scheduled scan tasks if a previously started scheduled scan is still running. Kaspersky Endpoint Security will enqueue scheduled scan tasks if the current scan continues. This helps optimize the load on the computer. For example, a scan task is scheduled to run at 6:00 PM and at 8:00 PM. The scan task that is scheduled to run at 8:00 PM is delayed if the 6:00 PM scan is still running. The delayed task is run after the 6:00 PM task finishes.	`Yes` to enqueue scheduled scan tasks if the current scan is still running. `No` (default value) to run scheduled scan tasks even if the current scan is still running.

Integration with Jenkins

Kaspersky Endpoint Security supports integration with Jenkins. Jenkins Pipeline plug-ins can be used to scan Docker images at different stages. For example, you can scan Docker images in a repository during the development process or before publishing.

To integrate Kaspersky Endpoint Security with Jenkins:

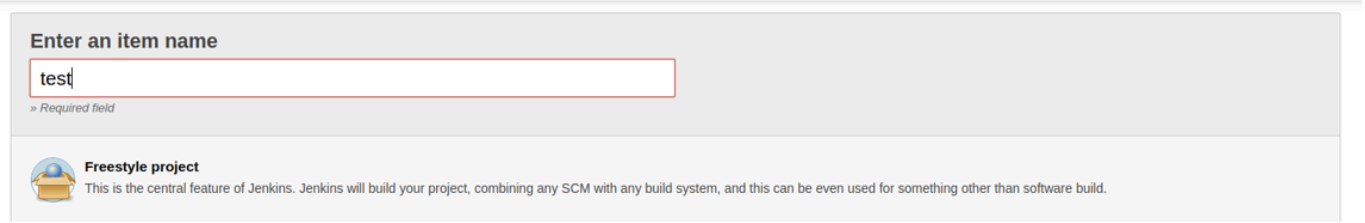
1. Install Kaspersky Endpoint Security on a Jenkins node.
2. Install Docker Engine on a Jenkins node.

   For details, please refer to the Docker Engine documentation.
3. Grant the Kaspersky Endpoint Security administrator privileges to the Jenkins user:

   ```
   kesl-control --grant-role admin <Jenkins user name>
   ```
4. Add a Jenkins user to the docker group:

   ```
   sudo usermod -aG docker <Jenkins user name>
   ```

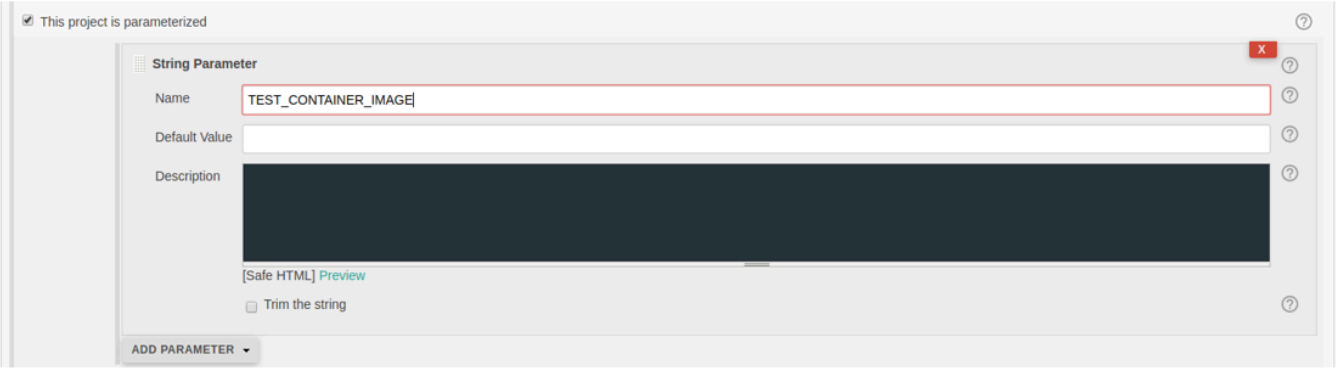
   Usually the jenkins name is used.
5. In Jenkins, create a new build job with the `test` name (**New Item** → **Enter an item name**).

6. Configure your project, according to your needs. It is assumed that as a result, you have an image or a started container that you need to scan.

7. To start the Docker container, add the following script to the Jenkins build procedure. If you use Jenkins plug-ins or another way to start Docker containers, save the ID of the running Docker container to the file /tmp/kesl_cs_info, for further scanning:

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
echo "Start container from image: '${TEST_CONTAINER_IMAGE}'"
CONTAINER_ID=$(docker run -d -v /storage:/storage ${TEST_CONTAINER_IMAGE} /storage/docker_process.sh)
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot start container from image ${TEST_CONTAINER_IMAGE}"
exit 1
fi
echo "${CONTAINER_ID}" > ${TMP_FILE}
exit ${EXIT_CODE}
```



8. After building the artifacts, add the following script to the steps to build the jenkins.

   This script supports one container for scanning. If necessary, modify the script according to your needs.

```
TMP_FILE="/tmp/kesl_cs_info"
EXIT_CODE=0
if [ ! -f "${TMP_FILE}" ] ; then
echo "Cannot find temporary file with container ID: '${TMP_FILE}'"
exit 1
fi
CONTAINER_ID=$(cat ${TMP_FILE})
if [ -z "${CONTAINER_ID}" ] ; then
echo "Cannot find container ID in the temporary file: '${TMP_FILE}'"
exit 1
fi
echo "Start anti-virus scan for: '${CONTAINER_ID}'"
THREATS_AMOUNT=$(kesl-control --scan-container ${CONTAINER_ID}|grep 'Total detected objects'|awk '{print $5}')
if [ "${THREATS_AMOUNT}" != "0" ] ; then
echo "ATTENTION! ${THREATS_AMOUNT} threats detected at: '${CONTAINER_ID}'"
EXIT_CODE=1
else
echo "Not threats found"
fi
echo "Remove container: {${CONTAINER_ID}}"
docker kill ${CONTAINER_ID}
docker rm -f ${CONTAINER_ID}
rm -f ${TMP_FILE}
```

9. To scan a Docker image from a repository, use the following script:

```
DOCKER_FILE=https://raw.githubusercontent.com/ianmiell/simple-dockerfile/master/Dockerfile
DOCKER_FILE_FETCHED=$$.Dockerfile
TEST_IMAGE_NAME=test_image
echo "Build image from ${DOCKER_FILE}"
curl ${DOCKER_FILE} -o ${DOCKER_FILE_FETCHED}
if [ -f ${DOCKER_FILE_FETCHED} ] ; then
echo "Dockerfile fetched: ${DOCKER_FILE_FETCHED}"
else
echo "Dockerfile not fetched"
exit 1
fi
docker build -f ${DOCKER_FILE_FETCHED} -t ${TEST_IMAGE_NAME}
echo "Scan docker image"
SCAN_RESULT=$(/opt/kaspersky/kesl/bin/kesl-control --scan-container ${TEST_IMAGE_NAME}*)
echo "Scan done: "
echo $SCAN_RESULT
```

10. Save the build job.

Anti-Cryptor task

In the command line, you can manage Anti-Cryptor using the Anti-Cryptor task (`Anti_Cryptor`).

By default, the Anti-Cryptor task does not run. You can start and stop this task manually.

You can configure Anti-Cryptor settings by editing the settings of the Anti-Cryptor predefined task.

Anti-Cryptor task settings

Setting	Description	Values
`ActionOnDetect`	Enables untrusted hosts blocking.	`Block` (default value) – enable untrusted hosts blocking. `Notify`: disable untrusted hosts blocking.
`BlockTime`	The time in minutes for which an untrusted device is blocked. If a compromised host is blocked, and you change a value for the `BlockTime` setting, the blocking time for this host will not change. The blocking time is not a dynamic value, and is calculated at the moment of blocking.	Integer from 1 to 4294967295. Default value: 30.
`UseExcludeMasks`	Enables exclusion of the objects specified by the `ExcludeMasks.item_#` setting from the protection scope. This setting applies only if the `ExcludeMasks.item_#` setting is specified.	`Yes` — Exclude the objects specified by the `ExcludeMasks.item_#` setting from the protection scope. `No` (default value) — Do not exclude the objects specified by the `ExcludeMasks.item_#` setting from the protection scope.
`ExcludeMasks.item_#`	Excludes objects from the protection scope by names or masks. You can use this setting to exclude an individual file from the specified protection scope by name or exclude multiple files at the same time using masks in the shell format. Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled. If you want to specify several masks, specify each mask on a new line with a new index.	The default value is not defined.
The **[ScanScope.item_#]** section contains the scopes protected by the application. For the Anti-Cryptor task, you need to specify at least one protection scope; you can only specify shared directories. You can specify several [ScanScope.item_#] sections in any order. The application processes the scopes by index in ascending order. The [ScanScope.item_#] section contains the following settings:		
`AreaDesc`	Description of protection scope; contains additional information about the protection scope.	Default value: `All shared directories`.

Setting	Description	Values
`UseScanArea`	Enables protection of the specified scope. To run the task, enable protection of at least one scope.	`Yes` (default value) — Protect the specified scope. `No` — Do not protect the specified scope.
`AreaMask.item_#`	Protection scope limitation. In the protection scope, the application protects only the objects that are specified using the masks in the shell format. You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	Default value: `*` (protect all objects).
`Path`	Path to the directory with the objects to be protected.	`< path to local directory >` – Protect a local directory accessible via SMB/NFS. You can use masks to specify the path. `AllShared` (default value) — Protect all resources accessible via SMB/NFS. `Shared:SMB` – Protect resources accessible via SMB. `Shared:NFS` – Protect resources accessible via NFS.
The **[ExcludedFromScanScope.item_#]** section contains the objects to be excluded from all [ScanScope.item_#] sections. The objects that match the rules of any [ExcludedFromScanScope.item_#] section are not scanned. The format of the [ExcludedFromScanScope.item_#] section is similar to the format of the [ScanScope.item_#] section. You can specify several [ExcludedFromScanScope.item_#] sections in any order. The application processes the scopes by index in ascending order. The [ExcludedFromScanScope.item_#] section contains the following settings:		
`AreaDesc`	Description of the protection exclusion scope, which contains additional information about the exclusion scope.	Default value: `All objects`.
`UseScanArea`	Excludes the specified scope from protection.	`Yes` (default value) — Exclude the specified scope from protection. `No` — Do not exclude the specified scope from protection.
`AreaMask.item_#`	Limitation of the protection exclusion scope. In the exclusion scope, the application excludes only the objects that are specified using masks in the shell format. You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	Default value: `*` (exclude all objects)
`Path`	Path to the directory with objects excluded from protection.	`< path to local directory >` — Exclude objects in the specified directory from protection. You can use masks to specify the path. `Mounted:NFS` – Exclude the remote directories mounted on a client device using the NFS protocol from protection. `Mounted:SMB` – Exclude the remote directories mounted on a client device using the Samba protocol from protection. `AllRemoteMounted` – Exclude all remote directories mounted on a client device using the Samba and NFS protocols from protection.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Behavior Detection task

You can manage application Behavior Detection in the operating system via the command line by using the Behavior Detection predefined task (`Behavior_Detection`).

The Behavior Detection task runs by default. You can start and stop the task manually.

You can configure Behavior Detection by editing the settings of the Behavior Detection predefined task.

Behavior Detection task setting

Setting	Description	Values
`UseTrustedPrograms`	Excluding processes from scans.	`Yes` – do not scan the activity of the indicated processes. `No` (default value) – scan all processes.
`TaskMode`	Action performed by the application when malicious activity is detected in the operating system.	`Block` (default value) – terminate the process of the application performing malicious activity. `Notify` – do not terminate the process performing malicious activity; only log detection of malicious activity in the event log.
TelemetrySource	Additional settings for the collection of telemetry sent to Detection and Response solutions when integrated with such. The `UseTelemetryMonopolyMode` setting is applied only if `TelemetrySource` is set to `Default`.	`Default` (default) means the eBPF technology and auditd service are used to get telemetry. `OnlyEBPF` means that only the eBPF technology is used to get telemetry.
UseTelemetryMonopolyMode	This setting is not applicable to devices with an Elbrus CPU.	`True` (default) means Kaspersky Endpoint Security uses the auditd service in exclusive mode. `False` means the auditd service is used in non-exclusive mode.
The **[TrustedPrograms.item_#]** section contains processes that are excluded from Behavior Detection scans. Kaspersky Endpoint Security does not monitor the activity of the specified processes.		
`ProgramPath`	Path to excluded process.	`< full path to process >` – Do not scan the process in the specified local directory. You can use masks to specify the path.
`ApplyToDescendants`	Exclude child processes of the excluded process specified by the `ProgramPath` setting from scans.	`Yes` – exclude the specified process and all its child processes from scans. `No` (default value) – exclude only the specified process from scans, do not exclude its child processes from scans.
`ProgramDesc`	Description of the excluded process.	
`UseTrustedProgram`	Exclude the activity of the specified process from scanning.	`Yes` (default value) – Exclude the activity of the specified process from scanning. `No` – do not exclude the activity of the specified process from scanning.

Setting	Description	Values
`UseTrustedProgramForDetects`	Excluding the activity of a process from scanning by Behavior Detection.	If set to `Yes`, the activity of the specified process is excluded from scanning by Behavior Detection. If set to `No` (default), the activity of the specified process is not excluded from scanning by Behavior Detection.
`UseTrustedProgramForMDRAndEDR`	Exclusion of the process from telemetry collected by the MDR and EDR Expert (on-premises) components. This setting is not applicable to devices with an Elbrus CPU.	`Yes` – exclude the activity of this process from telemetry collected by the MDR and EDR Expert (on-premises) components. `No` (default value) – do not exclude the activity of this process from telemetry.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Exploit Prevention

On the command line, you can manage Exploit Prevention using the settings of the Behavior Detection predefined task (`Behavior_Detection`).

You can configure Exploit Prevention by editing the settings of the Behavior Detection predefined task (see the table below).

Exploit Prevention settings

Setting	Description	Values
`UseAEP`	Enable the Exploit Prevention component.	`Yes` enables Exploit Prevention. `No` (default) disables Exploit Prevention.
`AEPMode`	The action to take when an exploit is detected.	If set to `Block` (default), malicious activity of the exploit is blocked and an event is logged. If set to `Notify`, the activity of the exploit is not blocked, only information about the exploit being detected is recorded in the event log.
The **[AEPExclusions.item_#]** section contains exclusions from scanning for the Exploit Protection component.		
`Enabled`	Enabling the exclusion from scanning of the Exploit Prevention protection component.	`Yes` (default value) – use the Exploit Prevention exclusion. `No` – do not use the Exploit Prevention exclusion.

Setting	Description	Values
`DetectName`	Excludes an object from scans by the name of the threat detected in the object. Before specifying a value for this setting, make sure that the `UseDetectName` setting is enabled.	In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected. You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com.
`Hash`	Excludes an object in which a threat was detected by its hash. Before specifying a value for this setting, make sure that the `UseHash` setting is enabled.	
`HashType`	The type of file hash that you want to use to exclude the file from scanning using the `Hash` parameter.	`Md5` – MD5 hash `Sha256` – SHA256 hash
`Path`	Excludes an object in which a threat was detected by its path. Before specifying a value for this setting, make sure that the `UsePath` setting is enabled.	`< full path to file or local directory >` – exclude the file or objects in the specified directory (including subdirectories) from scans. You can use the `*` and `?` characters in the path.
`UseDetectName`	Enables exclusion of objects containing the threats specified by the `DetectName` setting from scans.	`Yes` (default value) — exclude objects containing the threats specified by the `DetectName` setting from scans. `No` —Do not exclude from scanning the objects containing threats specified using the `DetectName` setting
`UseHash`	Exclude files with a detected threat by their hashes. The file hash is specified in the `Hash` parameter.	`Yes` (default value) – exclude a file with a detected threat by its hash. `No` – do not exclude a file with a detected threat by its hash.
`UsePath`	Exclude files with a detected threat by their paths. The path to the file is specified using the `Path` parameter.	`Yes` (default value) – exclude a file with a detected threat by its path. `No` – do not exclude a file with a detected threat by its path.

Using Kaspersky Security Network

You can enable or disable the use of Kaspersky Security Network in the command line by using the `UseKSN` option in the general application settings.

You can change the value of the `UseKSN` setting using command line options or a configuration file that contains all general application settings.

To enable the use of Kaspersky Security Network with the help of command line switches, run:

```
kesl-control --set-app-settings UseKSN=<Extended/Basic> --accept-ksn
```

where:

`<Extended/Basic>`: Kaspersky Security Network mode.

`--accept-ksn`: an option signifying that you agree to the terms in the Kaspersky Security Network Statement. You confirm that you have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement.

The file ksn_license.<language ID> containing the text of the Kaspersky Security Network Statement is located in the directory /opt/kaspersky/kesl/doc/.

To disable the use of Kaspersky Security Network with the help of command line switches, run:

```
kesl-control --set-app-settings UseKSN=No
```

To enable or disable use of Kaspersky Security Network with a configuration file, execute the following command:

```
kesl-control --set-app-settings --file <path to the configuration file> [--json] [--accept-ksn]
```

where:

`--file <path to the configuration file>` is the full path to the configuration file with general application settings where the required `UseKSN` value is configured.

Specify the `--json` option if you are importing settings from a JSON configuration file. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

`--accept-ksn`: an option signifying that you agree to the terms in the Kaspersky Security Network Statement. You must specify the option if you are enabling the use of Kaspersky Security Network.

If Kaspersky Endpoint Security installed on a client device runs under a Kaspersky Security Center policy, the value of the `UseKSN` setting can only be modified by using Kaspersky Security Center. When Kaspersky Endpoint Security installed on a client device stops running under a policy, the following value is assigned to the setting: `UseKSN=No`.

Connecting to Kaspersky Security Network

To check the connection to Kaspersky Security Network, run the following command:

```
kesl-control --app-info
```

The **Using Kaspersky Security Network** line displays the status of the connection to Kaspersky Security Network:

- If the *Extended KSN mode* status is displayed, Kaspersky Endpoint Security uses Kaspersky Security Network, information can be obtained from the knowledge base, and anonymous statistics and information about the types and sources of threats are sent.
- If the *Basic KSN mode* status is displayed, Kaspersky Endpoint Security uses Kaspersky Security Network and information can be obtained from the knowledge base, but anonymous statistics and information about the types and sources of threats are not sent.
- If the *KSN is not being used* status is displayed, Kaspersky Endpoint Security does not use Kaspersky Security Network.

The **Kaspersky Security Network Infrastructure** line displays information about the infrastructure solution that is used to work with Kaspersky reputation databases: *KSN* or *KPSN*.

A connection to Kaspersky Security Network may be absent for the following reasons:

- The user device is not connected to the internet.
- The use of Kaspersky Security Network is disabled.
- The application has not been activated or the license has expired.
- Problems related to the license key are detected. For example, the key is in the denylist.

Enabling or disabling cloud mode

Cloud mode is an operating mode of Kaspersky Endpoint Security that uses a lightweight version of the malware databases.

> If Kaspersky Endpoint Security is used in Light Agent mode for protecting virtual environments, use of the lightweight malware databases is not supported. The application receives special databases required for Light Agent operation from Protection Server.

You can enable or disable cloud mode in the command line with the help of the `CloudMode=Yes/No` option in the general application settings.

You can change the `CloudMode` setting using a configuration file that contains all general application settings, or using command line options.

> Cloud mode is available if use of Kaspersky Security Network is enabled.

BadUSB Attack Prevention task

On the command line, you can also manage BadUSB Attack Prevention using the BadUSB Attack Prevention predefined task (`Bad_USB`).

The BadUSB Attack Prevention task is not started by default. You can start and stop this task manually.

> Administrator role privileges are required to start and stop the BadUSB Attack Prevention task from the command line.

You can manage BadUSB Attack Prevention settings by editing the settings of the BadUSB Attack Prevention predefined task.

The following table describes available values and default values of settings that you can specify for the BadUSB Attack Prevention task.

BadUSB Attack Prevention task settings

Setting	Description	Values
`MaxAuthAttempts`	Maximum number of USB device authorization attempts after which the application blocks the USB device and further attempts to authorize the USB device for the duration specified in the `TimeoutAfterAttempts` parameter.	Possible values: 1 to 10 Default value: 5.
`TimeoutAfterAttempts`	USB device blocking duration after `MaxAuthAttempts` unsuccessful attempts to enter an authorization code.	Possible values: 1 to 180 minutes. Default value: 5 minutes.

Setting	Description	Values
`ProhibitOnScreenKeyboard`	Prohibit or allow the on-screen keyboard for authorizing USB devices.	If `Yes`, the application does not allow using the on-screen keyboard for keyboard authorization of a USB device that cannot be used to enter an authorization code. If `No`, the application allows using the on-screen keyboard for keyboard authorization of a USB device that cannot be used to enter an authorization code.
`ProhibitBarcodeScanner`	Enables or disables displaying the authorization code as a barcode for authorizing USB devices that do not make it possible to enter an authorization code.	`Yes` (default) prohibits displaying the authorization code as a barcode. `No` allows displaying the authorization code as a barcode.

Communication & Web Protection

Web Threat Protection task

In the command line, you can manage Web Threat Protection using the Web Threat Protection predefined task (`Web_Threat_Protection`).

The task starts automatically if one of the supported browsers is detected in the system and local management of Web Threat Protection settings is allowed on the device (a policy is not applied or the "lock" is not set in the policy properties). You can start and stop the task manually.

You can configure Web Threat Protection settings by editing the settings of the Web Threat Protection predefined task.

Web Threat Protection task settings

Setting	Description	Values
`ActionOnDetect`	Specifies the action to be performed upon detection of an infected object in web traffic.	`Notify` — Allow the detected object to be downloaded, display a notification about the blocked access attempt, and log information about the infected object. `Block` (default value) — Block access to the detected object, display a notification about the blocked access attempt, and log information about the infected object.
`CheckMalicious`	Checking links against the database of malicious web addresses.	`Yes` (default value) — Check if the links are listed in the malicious links database. `No` — Do not check if the links are listed in the malicious links database.
`CheckPhishing`	Checking links against the database of phishing web addresses.	`Yes` (default value) — Check if the links are listed in the phishing links database. `No` — Do not check if the links are listed in the phishing links database.
`UseHeuristicForPhishing`	Using heuristic analysis for scanning web pages for phishing links. This setting is not applicable to devices with an Elbrus CPU.	`Yes` (default value) — Use heuristic analysis to detect phishing links. If this value is specified, the level of heuristic analysis is `Light` (the least thorough scan with minimal load on the system). You cannot change the heuristic analysis level for the Web Threat Protection task. `No` — Do not use heuristic analysis to detect phishing links.

Setting	Description	Values
`CheckAdware`	Checking links against the database of advertising web addresses.	`Yes` — Check if the links are listed in the adware links database. `No` (default value) — Do not check if the links are listed in the adware links database.
`CheckOther`	Checking links against the database of web addresses containing legitimate applications that intruders can use to compromise the devices or data.	`Yes` —Check if the links are listed in the database of web addresses that contain legal applications that may be used by intruders to damage your devices or data. `No` (default value) — Do not check if the links are listed in the database of web addresses that contain legal applications that may be used by intruders to damage your devices or data.
`UseTrustedAddresses`	Using the list of trusted web addresses. The application does not scan trusted web addresses for viruses or other malicious objects. You can specify trusted web addresses using the `TrustedAddresses.item_#` setting.	`Yes` (default value) — Use a list of trusted web addresses. `No` — Do not use a list of trusted web addresses.
`TrustedAddresses.item_#`	Specifies trusted web addresses.	The default value is not defined. You can use masks to specify web addresses. Masks are not supported to specify IP addresses.

Useful articles

How to specify masks

When creating an address mask, use an asterisk (*) as a placeholder for one or more characters. If you enter the *abc* address mask, it is applied to all web resources that contain the "abc" sequence (for example, www.virus.com/download_virus/page_0-9abcdef.html). To include the asterisk in the address mask as a character, but not as a mask, enter the * character twice (for example, www.virus.com/**/page_0-9abcdef.html means www.virus.com/*/page_0-9abcdef.html).

Scanning network traffic

On the command line, you can use special management commands to manage network traffic scan settings. You can use network traffic scan settings management commands to:

- Manage network traffic scan settings.
- View exclusions from the encrypted connections scan.
- Clear the list of domains that the application automatically excluded from the scan.
- Configure the list of trusted root certificates that the application uses when scanning encrypted connections.
- Configure and view traffic interception exclusions.

Viewing and editing network traffic scan settings

You can use special network traffic scan settings management commands to:

- Output the current values of network traffic scan settings to the console or to a configuration file. You can use this file to edit the settings.
- Manage all network traffic scan settings using the configuration file. You can get a configuration file that you can edit using the display the network traffic scan settings output command.
- Edit individual settings using command line options in the format `< setting name >=< setting value >`. You can get the current values of the settings using the command to output network traffic scan settings.

To output the current network traffic scan settings to the console, execute the following command:

```
kesl-control --get-net-settings [--json]
```

Where `--json` is specified to output the settings in JSON format. If the `--json` option is not specified, the settings are output in the INI format.

To output the current network traffic scan settings to a file, run the following command:

```
kesl-control --get-net-settings --file <path to configuration file> [--json]
```

where:

- `--file <path to the configuration file>` is the path to the file where the network traffic scan settings will be saved. If you specify the name of a file without specifying its path, the file will be created in the current directory. If a file with the specified name already exists in the specified path, it will be overwritten. If the specified directory cannot be found on the disk, file will not be created.
- `--json` is specified to output the settings in JSON format. If the `--json` option is not specified, the settings are output in the INI format.

To manage network scan settings using a configuration file:

1. Output the network traffic scan settings to the configuration file, as described above.
2. Edit the values of the necessary parameters in the file and save the changes.
3. Run the following command:

   ```
   kesl-control --set-net-settings --file <path to the configuration file> [--json]
   ```

where:

- `--file <path to the configuration file>` is the full path to the configuration file with the network traffic scan settings.
- `--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` option is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

All network traffic scan settings configured in the file are imported into the application.

To edit network traffic scan settings on the command line, run the following command:

```
kesl-control --set-net-settings <parameter name>=<parameter value> [<parameter name>=<parameter value>]
```

where `<parameter name>=<parameter value>` is the name and value of a network traffic scan setting.

The values of the specified settings are modified.

Viewing exclusions from encrypted connections scan

You can view the following lists of exclusions from the encrypted connections scan:

- a list of exclusions added by the user;
- a list of exclusions added by the application;
- list of exclusions received from the application databases.

To view the list of encrypted connection scan exclusions added by a user, execute the following command:

```
kesl-control -N --query user
```

To view the list of encrypted connection scan exclusions added by a user, execute the following command:

```
kesl-control -N --query auto
```

To view the list of encrypted connection scan exclusions received from the application databases, execute the following command:

```
kesl-control -N --query kl
```

To clear a list of domains that the application automatically excluded from scan, execute the following command:

```
kesl-control [-N] --clear-web-auto-excluded
```

Managing the list of trusted root certificates

To add a certificate to the list of trusted root certificates, run the following command:

```
kesl-control --add-certificate <path to the certificate>
```

where:

`<path to the certificate>` is the path to the certificate file that you want to add (in PEM or DER format).

To remove a certificate from the list of trusted root certificates, run the following command:

```
kesl-control --remove-certificate <subject of the certificate>
```

To view the list of trusted root certificates, execute the following command:

```
kesl-control --list-certificates
```

The following information is displayed for each certificate:

- Certificate subject
- serial number
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA256 certificate fingerprint

Configuring and viewing traffic interception exclusions

To add a traffic interception exclusion, run the following command:

```
kesl-control --add-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port <destination
port>
```

where:

- `<in|out>` is the direction of traffic in the excluded connection. You can configure an exclusion for inbound traffic or for outbound traffic.
- `<remote IP address>` is the IPv4 or IPv6 address of the remote device. Depending on the traffic direction, traffic coming from the specified IP address (exclusion for inbound traffic) or traffic going to the specified IP address (exclusion for outgoing traffic) is excluded.

- `<destination port>` is, depending on the direction of traffic:
  - Port on the protected device (exclusion for inbound traffic). Traffic to this port from remote devices is excluded from interception.
  - Port on the remote device (exclusion for outbound traffic). Traffic to this port from the protected device is excluded from interception.

In an exclusion, you may specify an IP address of the remote device without a port or a destination port without an IP address.

> If you specify only the IP address of the remote device in an exclusion for inbound traffic (without specifying a port on the protected device), all traffic from the remote device is excluded from interception. We recommend configuring this exclusion only for traffic from devices that you trust.

To view the list of configured traffic interception exclusions, run the following command:

```
kesl-control --list-bypass-endpoints
```

The following information is displayed for each exclusion:

- Serial number of the exclusion
- Direction of traffic
- IP address of the remote device
- Port number

To delete a traffic interception exclusion, run the following command:

```
kesl-control --remove-bypass-endpoints --direction <in|out> --remote-ip <remote IP address> --dst-port
<destination port>
```

where:

- `<in|out>` is the direction of traffic in the excluded connection.
- `<remote IP address` is the IPv4 or IPv6 address of the remote device whose traffic is excluded from interception (depending on the direction of traffic).
- `<destination port>` is a port on the protected device (exclusion for inbound traffic) or a port on the remote device (exclusion for outbound traffic).

Network Threat Protection task

In the command line, you can manage Network Threat Protection using the Network Threat Protection predefined task (`Network_Threat_Protection`).

By default, the Network Threat Protection task does not run. You can start and stop the task manually.

You can configure Network Threat Protection settings by editing the settings of the Network Threat Protection predefined task.

Network Threat Protection task settings

Setting	Description	Values
`ActionOnDetect`	Action performed when network activity typical of network attacks is detected. Changing the value of this setting from `Block` to `Notify` clears the list of blocked devices.	`Notify` – allow network activity, log information about detected network activity. If this value is specified, the value of the `BlockAttackingHosts` parameter is ignored. `Block` (default value) – block network activity and log information about it.
`BlockAttackingHosts`	Blocking network activity from attacking devices.	`Yes` (default value) — Block network activity of an attacking device. `No` – Do not block network activity of the attacking device. If this value is specified and the `ActionOnDetect` parameter is set to `Block`, the application blocks network activity from the attacking device, but does not add the device to the list of blocked devices.
`BlockDurationMinutes`	Specifies how long attacking devices will be blocked (in minutes).	1 to 32768 Default value: 60.
`UseExcludeIPs`	The usage of a list of IP addresses whose network activity will not be blocked when a network attack is detected. The application will only log information about dangerous activity from these devices. You can add IP addresses to the exclusion list by using the `ExcludeIPs.item_#` setting.	`Yes` — Use the list of excluded IP addresses. `No` (default value) — Do not use the list of excluded IP addresses.
`ExcludeIPs.item_#`	Specifies an IP address whose network activity will not be blocked by the application. By default, the list is empty.	`d.d.d.d` — IPv4 address, where d is a decimal number from 0 to 255. `d.d.d.d/p` — Subnet of IPv4 addresses, where p is a number from 0 to 32. `x:x:x:x:x:x:x:x` — IPv6 address, where x is a hexadecimal number from 0 to ffff. `x:x:x:x::0/p` — Subnet of IPv6 addresses, where p is a number from 0 to 64. The default value is not defined.

Firewall Management

In the command line, you can configure Firewall Management using the Firewall Management predefined task (`Firewall_Management`).

By default, the Firewall Management Task is not run. You can start and stop this task manually.

You can configure the firewall management settings by editing the settings of the Firewall Management predefined task.

You can also configure Firewall Management settings using Firewall Management commands:

- Create and delete network packet rules and change their execution priority.
- Create a list of IP addresses or subnets in network zones.
- View firewall rules created in the application by using the following command:

```
kesl-control -F --query
```

Setting	Description	Values
`DefaultIncomingAction`	The default action to perform on an inbound connection if no network rules apply to this connection type.	`Allow` (default value) — Allow inbound connections. `Block` — Block inbound connections.
`DefaultIncomingPacketAction`	The default action to perform on an incoming packet if no network packet rules apply to this connection type.	`Allow` (default value) — Allow incoming packets. `Block` — Block incoming packets.
`OpenNagentPorts`	Adds Network Agent dynamic rules to the network packet rules.	`Yes` (default value) – Add Network Agent dynamic rules to the network packet rules. `No` – Do not add Network Agent dynamic rules to the network packet rules.
The **[PacketRules.item_#]** section contains network packet rules for the Firewall Management task. You can specify several `[PacketRules.item_#]` sections in any order. The application processes the scopes by index in ascending order. Each `[PacketRules.item_#]` section contains the following settings:		
`Name`	Network packet rule name.	Default value: `Packet rule #<n>`, where n is an index.
`FirewallAction`	Action to be performed on connections specified in this network packet rule.	`Allow` (default value) — Allow network connections. `Block` — Block network connections.

`Protocol`	Type of protocol for which network activity is to be monitored.	`Any` (default value) — The Firewall Management task monitors all network activity.
		`TCP`
		`UDP`
		`ICMP`
		`ICMPv6`
		`IGMP`
		`GRE`

`RemotePorts`	Port numbers of the remote devices whose connection is monitored. An integer or interval can be specified for this value. This setting can only be specified if the `Protocol` setting is set to `TCP` or `UDP`.	`Any` (default value) — Monitor all remote ports. `0 – 65535`.
`LocalPorts`	Port numbers of the local devices whose connection is monitored. An integer or interval can be specified for this value. This setting can only be specified if the `Protocol` setting is set to `TCP` or `UDP`.	`Any` (default value) — Monitor all local ports. `0 – 65535`.
`ICMPType`	ICMP packet type. This setting can only be specified if the `Protocol` setting is set to `ICMP` or `ICMPv6`.	`Any` (default value) — Monitor all ICMP packet types. Integer number according to the data transfer protocol specification.
`ICMPCode`	ICMP packet code. This setting can only be specified if the `Protocol` setting is set to `ICMP` or `ICMPv6`.	`Any` (default value) — Monitor all ICMP packet codes. Integer number according to the data transfer protocol specification.
`Direction`	Direction of the monitored network activity.	`IncomingOutgoing` or `InOut` (default value) — Monitor both inbound and outbound connections. `Incoming` or `In` — Monitor only inbound connections. `Outgoing` or `Out` — Monitor only outbound connections. `IncomingPacket` or `InPacket` — Monitor only incoming packets. `OutgoingPacket` or `OutPacket` — Monitor only outgoing packets. `IncomingOutgoingPacket` or `InOutPacket` — Monitor both incoming and outgoing packets.

Setting	Description	Values
`RemoteAddress`	The network addresses of the remote devices that can send and receive network packets.	`Any` (default value) — Monitor network packets sent and/or received by remote devices with any IP address. `Trusted` — Predefined network zone for trusted networks. `Local` — Predefined network zone for local networks. `Public` — Predefined network zone for public networks. `d.d.d.d` — IPv4 address, where d is a decimal number from 0 to 255. `d.d.d.d – d.d.d.d` — Range of IPv4 addresses. `d.d.d.d/p` — Subnet of IPv4 addresses, where p is a number from 0 to 32. `x:x:x:x:x:x:x:x` — IPv6 address, where x is a hexadecimal number from 0 to ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` — Range of IPv6 addresses. x:x:x:x:x:x:x:x/p — Subnet of IPv6 addresses, where p is a number from 0 to 128; you can use **::** for brevity.
`LocalAddress`	Network addresses of devices that have Kaspersky Endpoint Security installed and can send and/or receive network packets.	`Any` (default value) — Monitor network packets sent and/or received by local devices with any IP address. `d.d.d.d` — IPv4 address, where d is a decimal number from 0 to 255. `d.d.d.d – d.d.d.d` — Range of IPv4 addresses. `d.d.d.d/p` — Subnet of IPv4 addresses, where p is a number from 0 to 32. `x:x:x:x:x:x:x:x` — IPv6 address, where x is a hexadecimal number from 0 to ffff. `x:x:x:x:x:x:x:x – x:x:x:x:x:x:x:x` — Range of IPv6 addresses. x:x:x:x:x:x:x:x/p — Subnet of IPv6 addresses, where p is a number from 0 to 128; you can use **::** for brevity.
`LogAttempts`	Include a record of the network rule action in the report.	`Yes` — Log actions in the report. `No` (default value)—Do not write the actions in the report.
The **[NetworkZonesPublic]** section contains network addresses associated with public networks. You can specify several IP addresses or subnets of IP addresses.		
`Address.item_#`	Specifies IP addresses or subnets of IP addresses.	`d.d.d.d` — IPv4 address, where d is a decimal number from 0 to 255. `d.d.d.d/p` — Subnet of IPv4 addresses, where p is a number from 0 to 32. `x:x:x:x:x:x:x:x` — IPv6 address, where x is a hexadecimal number from 0 to ffff. `x:x:x:x::0/p` — Subnet of IPv6 addresses, where p is a number from 0 to 64. Default value: "" (no network addresses in this zone)
The **[NetworkZonesLocal]** section contains network addresses associated with local networks. You can specify several IP addresses or subnets of IP addresses.		
`Address.item_#`	Specifies IP addresses or subnets of IP addresses.	`d.d.d.d` — IPv4 address, where d is a decimal number from 0 to 255. `d.d.d.d/p` — Subnet of IPv4 addresses, where p is a number from 0 to 32. `x:x:x:x:x:x:x:x` — IPv6 address, where x is a hexadecimal number from 0 to ffff. `x:x:x:x::0/p` — Subnet of IPv6 addresses, where p is a number from 0 to 64. Default value: `""` (no network addresses in this zone)

Setting	Description	Values
The **[NetworkZonesTrusted]** section contains network addresses associated with trusted networks. You can specify several IP addresses or subnets of IP addresses.		
`Address.item_#`	Specifies IP addresses or subnets of IP addresses.	`d.d.d.d` — IPv4 address, where d is a decimal number from 0 to 255. `d.d.d.d/p` — Subnet of IPv4 addresses, where p is a number from 0 to 32. `x:x:x:x:x:x:x:x` — IPv6 address, where x is a hexadecimal number from 0 to ffff. `x:x:x:x::0/p` — Subnet of IPv6 addresses, where p is a number from 0 to 64. Default value: `""` (no network addresses in this zone)

Configuring the list of network packet rules

To add a network packet rule, execute the following command:

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <Allow|Block>] [--protocol <protocol>] [--direction
<direction>] [--remote <remote address>:<port>] [--local <local address>:<port>] [--at <index>]
```

where:

- `--name <rule name>` is the name of the network packet rule.
- `--action <Allow|Block>` is the action to be performed on connections specified in this network packet rule.
- `--protocol <protocol>` is the protocol for which you want to monitor network activity.
- `--direction <direction>` is the direction of the monitored network activity.
- `--remote <remote address>:<port>` is the network address of the remote device. You can specify the name of a predefined network zone as the remote address.
- `--local <local address>:<port>` is the network address of the device with Kaspersky Endpoint Security installed.
- `--at <index>` is the index of the rule in the list of network packet rules. If the `--at` option is not specified or its value is larger than the number of rules in the list, the new rule is added to the end of the list.

Parameters that you do not specify values for in the command are set to their default values.

Example of creating a rule that blocks all incoming and established connections to TCP port 23

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
any
```

Example of creating a rule that blocks incoming and established connections via the TCP port 23 for the Public network zone

```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol TCP --local any:23 --remote
Public
```

To delete a network packet rule, execute one of the following commands:

```
kesl-control --del-rule --name <rule name>
```

or

```
kesl-control --del-rule --index <current index>
```

where:

- `--name <rule name>` is the name of the network packet rule.
- `--index <current index>` is the current index of rules in the list of network packet rules.

If the list of network packet rules contains multiple rules with an identical name or does not contain a rule with a specified name or index, an error occurs.

To change a network packet rule's execution priority, execute one of the following commands:

```
kesl-control --move-rule --name <rule name> --at < new index>
```

or

```
kesl-control --move-rule --index <current index> --at <new index>
```

where:

- `--name <rule name>` is the name of the network packet rule.
- `--index <current index>` is the current index of rules in the list of network packet rules.
- `--at <new index>` is the new index of rules in the list of network packet rules.

Configuring network zones

To add a network address to the zone, execute the following command:

```
kesl-control --add-zone <zone> --address <address>
```

where:

- `<zone>` is the predefined name of the network zone. Possible values: `Public`, `Local`, `Trusted`.
- `<address>` is the network address or subnet.

To delete a network address from a zone, execute one of the following commands:

```
kesl-control --del-zone <zone> --address <address>
```

or

```
kesl-control --del-zone <zone> --index <address index in the zone>
```

If a zone contains several items with the same network address, the `--del-zone` command will not be executed.

If the specified network address or index does not exist, an error message is generated.

Security Controls

Device Control task

The table describes all possible values and the default values of all the settings that you can specify for the Device Control task (`Device_Control`).

Device Control task settings

Setting	Description	Values
`OperationMode`	Response to attempts to access a device that is restricted according to Device Control rules.	`Block` (default value) – the application applies the access mode defined for the device or bus. `Notify` – the application tests the selected access mode and generates an event about the detection of an attempt to access a device.
`AllowToRequestTemporaryAccess`	Allow requesting temporary access to a blocked device. Granting access to a blocked device is available only if Kaspersky Security Center 16.1 is deployed in the organization and the client device is able to establish a connection with the Administration Server.	`Yes` – allow the user to request temporary access to the blocked device in the graphical interface of the application or on the command line. `No` (default) – do not allow the user to request temporary access to a blocked device.
The **[DeviceClass]** section contains access modes for devices depending on their type.		
`HardDrive`	Access mode for the hard drives connected to a client device.	`Allow` — Users are allowed access to hard drives. `DependsOnBus` (default): access to the hard drive depends on the access mode defined for the bus through which it is connected. `Block` — Access to all hard drives (except system hard drives, which are never blocked by the Device Control) is blocked for users. `ByRule` — Access to the hard drives depends on the access rules. `ReadOnly` — Users have read only access to hard drives, writing is blocked.

Setting	Description	Values
`RemovableDrive`	Access mode for the removable drives connected to a client device.	`Allow` — Access to the removable drives is allowed for users. `DependsOnBus` (default): access to the removable drive depends on the access mode defined for the bus through which it is connected. `Block` — Access to the removable drives is blocked for users. `ByRule` — Access to the removable drives depends on the access rules. `ReadOnly` — Users have read only access to removable drives, writing is blocked.
`FloppyDrive`	Access mode for the floppy disk drives connected to a client device. The application does not block floppy disk drives connected to the client device using the ISA bus.	`Allow` — Users are allowed access to floppy disk drives. `DependsOnBus` (default): access to the floppy disk drive depends on the access mode defined for the bus through which it is connected. `Block` — Access to floppy disk drives is blocked for users. `ByRule` — Access to floppy disk drives depends on the access rules. `ReadOnly` — Users have read only access to floppy disk drives, writing is blocked.
`OpticalDrive`	Access mode for the CD/DVD drives connected to a client device.	`Allow` — Users are allowed access to CD/DVD drives. `DependsOnBus` (default): access to the CD/DVD drive depends on the access mode defined for the bus through which it is connected. `Block` — Access to CD/DVD drives is blocked for users. `ByRule` — Access to CD/DVD drives depends on the access rules. `ReadOnly` — Users have read only access to CD/DVD drives, writing is blocked.
`SerialPortDevice`	Access mode for the devices connected to a client device via a serial port. The application does not block the devices connected to a client device via a serial port using the ISA bus.	`Allow` — Users are allowed access to devices connected through a serial port. `DependsOnBus` (default): access to a device connected through a serial port depends on bus access mode. `Block` — Access to devices connected through a serial port is blocked for users.
`ParallelPortDevice`	Access mode for the devices connected to a client device via a parallel port.	`Allow` — Users are allowed access to devices connected through a parallel port. `DependsOnBus` (default): access to a device connected through a parallel port depends on bus access mode. `Block` — Access to devices connected through a parallel port is blocked for users.
`Printer`	Access mode for the printers connected to a client device.	`Allow` — Users are allowed access to printers. `DependsOnBus` (default): access to a printer depends on the access mode defined for the bus through which it is connected. `Block` — Access to printers is blocked for users.
`Modem`	Access mode for the modems connected to a client device.	`Allow` — Users are allowed access to modems. `DependsOnBus` (default): access to a modem depends on the access mode defined for the bus through which it is connected. `Block` — Access to modems is blocked for users.
`TapeDrive`	Access mode for the tape devices connected to a client device.	`Allow` — Users are allowed access to tape devices. `DependsOnBus` (default): access to a tape device depends on the access mode defined for the bus through which it is connected `Block` — Access to tape devices is blocked for users.

Setting	Description	Values
`MultifuncDevice`	Access mode for the multifunctional devices connected to a client device.	`Allow` — Users are allowed access to multifunctional devices. `DependsOnBus` (default): access to a multifunctional device depends on the access mode defined for the bus through which it is connected. `Block` — Access to multifunctional devices is blocked for users.
`SmartCardReader`	Access mode for the smart card readers connected to a client device.	`Allow` — Access to smart card readers is allowed for users. `DependsOnBus` (default): access to a smart card reader depends on the access mode defined for the bus through which it is connected. `Block` — Access to smart card readers is blocked for users.
`WiFiAdapter`	Access mode for the Wi-Fi adapters connected to a client device.	`Allow` — Users are allowed access to Wi-Fi adapters. `DependsOnBus` (default): access to a Wi-Fi adapter depends on connection bus access mode. `Block` — Access to the Wi-Fi adapters is blocked for users.
`NetworkAdapter`	Access mode for the external network adapters connected to a client device.	`Allow` — Users are allowed access to external network adapters. `DependsOnBus` (default): access to an external network adapter depends on the access mode defined for the bus through which it is connected. Device Control does not allow denying access to external network adapters to avoid disconnecting the client device from the network.
`PortableDevice`	Access mode for the portable devices connected to a client device.	`Allow` — Users are allowed access to portable devices. `DependsOnBus` (default): access to a portable device depends on the access mode defined for the bus through which it is connected. `Block` — Access to portable devices is blocked for users.
`BluetoothDevice`	Access mode for the Bluetooth devices connected to a client device.	`Allow` — Users are allowed access to Bluetooth devices. `DependsOnBus` (default): access to a Bluetooth device depends on the access mode defined for the bus through which it is connected. `Block` — Access to Bluetooth devices is blocked for users.
`ImagingDevice`	Access mode for the imaging devices connected to a client device.	`Allow` —Access to all imaging devices is allowed for users. `DependsOnBus` (default): access to an imaging device depends on the access mode defined for the bus through which it is connected. `Block` —Access to all imaging devices is blocked for users.
`SoundAdapter`	Access mode for the sound adapters connected to a client device.	`Allow` —Access to all sound adapters is allowed for users. `DependsOnBus` (default): access to a sound adapter depends on the access mode defined for the bus through which it is connected. `Block` —Access to all sound adapters is blocked for users.
`InputDevice`	Access mode for the input devices (keyboards, mouse, touchpad, and others) connected to a client device.	`Allow` — Users are allowed access to input devices. `DependsOnBus` (default): access to an input device depends on the access mode defined for the bus through which it is connected. `Block` — Access to input devices is blocked for users.
The **[DeviceBus]** section contains access modes for connection buses.		

Setting	Description	Values
`USB`	Access mode for devices connected to the client device via USB.	`Allow` (default value) — Users are allowed access to USB-devices. `Block` — Access to USB-devices is blocked for users.
`FireWire`	Access mode for devices connected to the client device via FireWire.	`Allow` (default value) — Users are allowed access to devices connected via the FireWire interface. `Block` — Access to devices connected via the FireWire interface is blocked for users.
The **[TrustedDevices.item_ #]** section contains trusted devices.		
`DeviceId`	Specifies ID or ID mask of a trusted device.	You can use the masks * (any sequence of characters) or ? (any single character) to indicate the device ID. Examples: *To deny access to all USB devices except the specified one, specify the following settings:* In the `[DeviceBus]` section, specify `USB=Block` In the `[TrustedDevices.item_#]` section, specify `DeviceId=<device ID>` *To deny access to all USB devices, but allow access to all USB drives, specify the following settings:* In the `[DeviceBus]` section, specify `USB=Block` In the `[TrustedDevices.item_#]` section, specify `DeviceId=USBSTOR*`
`Comment`	Comment to the specified trusted device.	—
The **[TrustedDevices.item_#.Principals.item_#]** section contains the rules for accessing a trusted device.		
`Principal`	The user or group for which the device is trusted. If the device has the "read-only" access type, when the trusted device is assigned to a specific user, the assigned user is ignored and the device is made available for writing to all users.	`\Everyone` (default): the device is trusted for all users. `<user name>` is the name of a local or domain user for whom the device is trusted (without specifying the full name with the domain, if the system allows entering user names in this format, or in the <domain name>\`<user name>` or `<user name>`@<domain name> format). `@<group name>` is the name of the (local or domain) group of users for which the device is trusted.
The **[Schedules.item_#]** section contains the device access schedule. You can configure a schedule only for hard drives, removable drives, floppy disk drives, and CD/DVD drives.		
`ScheduleName`	Specifies a schedule name. The schedule name must be unique.	Default value: `Default`. The `Default` schedule provides users full access to devices at any time if the connection bus is allowed to access the corresponding device type. You cannot delete the `Default` schedule.

Setting	Description	Values
DaysHours	Specifies time intervals for a schedule.	All (default value) — The schedule is valid 24/7 (no time limitation). <weekday> – Days of the week. You can use either the full week day names or abbreviations (for example, for Monday, you can specify Mo, or Mon, or Monday). For week days, you can specify intervals or specific days. The week starts from Sunday. <hour> – Hours [0:24]. For hours, you can specify only intervals. Example of schedule_1, which is valid from Sunday till Saturday from 0 a.m. to 11 a.m., from 12 p.m. to 3 p.m., and from 4 p.m. to 12 a.m. [Schedules.item_0001] ScheduleName=schedule_1 DaysHours=Su-Sa:0..11,12..15,16..24 Example of schedule_2, which is valid for the following intervals: on Thursdays from 12 p.m. to 2 p.m. and on Fridays from 2 a.m. to 3 p.m. and from 4 p.m. to 12 a.m. [Schedules.item_0002] ScheduleName=schedule_2 DaysHours=Th:12..14;Fr:2..15,16..24 Example of schedule_3, which is valid 24 hours 7 days a week [Schedules.item_0003] ScheduleName=schedule_3 DaysHours=All
The **[HardDrivePrincipals.item_#]** section contains hard drive access rules. For hard drives, at least one schedule must always be enabled. You can assign several access rules to a hard drive. Also, multiple schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or group, the minimum access rights are granted.		
Principal	Specifies a user or group of users for whom the access rule is applied.	\Everyone (default value) is the access rule applies to all users. <user name> is the name of the local user to whom the access rule applies. @<group name> is the name of the group of users to which the access rule applies.
[HardDrivePrincipals.item_#.AccessRules.item_#] contains access rule settings.		
UseRule	Specifies whether the rule is enabled or disabled.	Yes (default value) — The access rule is enabled. No — The access rule is disabled.
ScheduleName	Schedule specified in the [Schedules.item_#] section.	Default value: Default.
Access	Specifies access type.	Allow (default value) — Access to hard drives is allowed. Block — Access to hard drives is blocked.
The **[RemovableDrivePrincipals.item_#]** section contains the access rules for removable drives. For removable drives, at least one schedule must always be enabled. You can assign several access rules to a removable drive. Also, multiple schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or group, the minimum access rights are granted.		
Principal	Specifies a user or group of users for whom the access rule is applied.	\Everyone (default value) is the access rule applies to all users. <user name> is the name of the local user to whom the access rule applies. @<group name> is the name of the group of users to which the access rule applies.
[RemovableDrivePrincipals.item_#.AccessRules.item_#] contains access rule settings.		
UseRule	Specifies whether the rule is enabled or disabled.	Yes (default value) — The access rule is enabled. No — The access rule is disabled.
ScheduleName	Schedule specified in the [Schedules.item_#] section.	Default value: Default.
Access	Specifies access type.	Allow (default value) — Access to removable drives is allowed. Block — Access to removable drives is blocked.

Setting	Description	Values
The **[FloppyDrivePrincipals.item_#]** section contains access rules for floppy drives. For floppy drives, at least one schedule must always be enabled. You can assign several access rules to a floppy drive. Also, multiple schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or group, the minimum access rights are granted.		
`Principal`	Specifies a user or group of users for whom the access rule is applied.	`\Everyone` (default value) is the access rule applies to all users. `<user name>` is the name of the local user to whom the access rule applies. `@<group name>` is the name of the group of users to which the access rule applies.
`[FloppyDrivePrincipals.item_#.AccessRules.item_#]` contains access rule settings.		
`UseRule`	Specifies whether the rule is enabled or disabled.	`Yes` (default value) — The access rule is enabled. `No` — The access rule is disabled.
`ScheduleName`	Schedule specified in the `[Schedules.item_#]` section.	Default value: `Default`.
`Access`	Specifies access type.	`Allow` (default value) — Access to floppy drives is allowed. `Block` — Access to floppy drives is blocked.
The **[OpticalDrivePrincipals.item_#]** section contains the access rules for CD/DVD drives. For CD/DVD drives, at least one schedule must always be enabled. You can assign several access rules to a CD/DVD drive. Also, multiple schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or group, the minimum access rights are granted.		
`Principal`	Specifies a user or group of users for whom the access rule is applied.	`\Everyone` (default value) is the access rule applies to all users. `<user name>` is the name of the local user to whom the access rule applies. `@<group name>` is the name of the group of users to which the access rule applies.
`[OpticalDrivePrincipals.item_#.AccessRules.item_#]` contains access rule settings.		
`UseRule`	Specifies whether the rule is enabled or disabled.	`Yes` (default value) — The access rule is enabled. `No` — The access rule is disabled.
`ScheduleName`	Schedule specified in the `[Schedules.item_#]` section.	Default value: `Default`.
`Access`	Specifies access type.	`Allow` (default value) — Access to CD/DVD drives is allowed. `Block` — Access to CD/DVD drives is blocked.

Web Control

On the command line, you can manage Web Control using the Web Control predefined task (`Web_Control`).

The Web Control task is stopped by default. You can start and stop the task manually.

You can edit Web Control settings by changing the settings of the Web Control predefined task.

You can also view and edit Web Control settings using Web Control management commands.

Web Control task

The table below describes all available values and the default values of all the settings that you can specify for the Web Control task (`Web_Control`).

Setting	Description	Values
`WebControlDefaultAction`	The default rule, that is, the action that Web Control performs when it detects an attempt to gain access to web resources that are not covered by other rules.	`Allow` (default value) – allow access to the web resources. `Block` – block access to the web resources.
`ComplaintRecipient`	The administrator's email address to which messages about mistaken blocking of web resources are sent.	
The **[Rules.item_#]** section contains the following settings:		
`Name`	Web resource access rule name. The rule name must be unique.	
`WebControlAction`	The action of the rule that Web Control will perform when it detects an attempt to access a web resource that matches the rule.	`Allow` (default value) – allow access to the web resource. `Block` – block access to the web resource. `Notify` – display a warning that the web resource is undesirable. By clicking links in the warning message, the user can access the requested web resource.
`Enabled`	Status of the web resource access rule.	`Yes` – the rule is enabled, Web Control applies this rule during operation. `No` (default value) – the rule is disabled and is not used when Web Control is running.
`ScheduleId`	Schedule ID that is used in the `[Schedules.item_#]` section.	
`UseUrls`	Use of a web resource address filter in a rule.	`Yes` – use a web resource address filter in the rule. `No` (default value) – do not use a web resource address filter, apply the rule to all web resource addresses.
`Urls.item_#`	The address of the web resource for which the rule controls access.	You can use masks to specify the web resource address.
`UseCategories`	Use of filters by content categories and data type categories in the rule.	`None` (default) – do not use a web resource content filter. `ContentOnly` – use the content category filter in the rule. `FormatOnly` – use the data type category filter in the rule. `ContentAndFormat` – use the content category filter and the data type category filter in the rule.
`[Rules.item_#.ContentCategories.item_#]`	Section for specifying the content category.	–

Setting	Description	Values
`ContentCategory`	Content categories.	`AdultContent`, `AlcoholTobaccoNarcotics`, `Violence`, `Profanity`, `Weapons`, `ChatForum`, `WebMail`, `OnlineShops`, `SocialNets`, `Recruitment`, `HttpQueryRedirection`, `CreditCards`, `PoliceDecision`, `SoftwareAudioVideo`, `TechnologyElectronics`, `GamblingLotteriesSweepstakes`, `InternetCommunicationMedia`, `CryptocurAndMining`, `LegislationBE`, `ECommerce`, `ComputerGames`, `Religions`, `News`, `Torrents`, `FileSharing`, `AudioAndVideo`, `BankSites`, `Blogs`, `DatingSites`, `LegislationRF`, `LegislationGlobal`, `SexuallyExplicit`, `Sexuality`, `AITools`
`[Rules.item_#.FormatCategories.item_#]`	Section for specifying the data type category.	–
`FormatCategory`	Data type category.	`Video` – Video `Audio` – Audio data `OfficeDocument` – Office application files `Executable` – Executable files `Archives` – Archives `Images` – Image files `Scripts` – Scripts
`UsePrincipals`	Use of a filter of users that are covered by the web resource access rule.	`Yes` – use the user filter in the rule. `No` (default value) – do not use the user filter, apply the rule to all users.
`[Rules.item_#.Principals.item_#]`	Section for specifying users that are covered by the web resource access rule.	
`Name`	User or group of users that is covered by the web resource access rule.	`<username>` is the name of the user to which the rule applies. `@<groupname>` is the name of the group of users to which the rule applies. Default value: The web resource access rule is applied for all users.
The **[UrlCategories.item_#]** section contains the following settings:		
`Name`	Name of the group of web resource addresses to which the rule controls access.	
`Urls.item_#`	Address of a web resource that belongs to the group.	You can use masks to specify the web resource address.
The **[Schedules.item_#]** section contains the rule schedule.		
`Id`	Schedule ID that is used in the `[Rules.item_#]` section.	`1 - 999999` `0` is the ID of the `Default` schedule which lets the rule work without any time limits, that is, at all times.

Setting	Description	Values
`Name`	Specifies a schedule name.	
`DaysHours`	Specifies time intervals for a schedule.	`<weekday>` – Days of the week. You can use either the full week day names or abbreviations (for example, for Monday, you can specify `Mo`, or `Mon`, or `Monday`). For week days, you can specify intervals or specific days. The week starts from Sunday. `<hour>` – Hours [0:24]. You can specify only intervals for hours.

Viewing and editing Web Control settings

To view Web Control settings, run the following command:

```
kesl-control --get-settings 26 [--file <path to the configuration file>] [--json]
```

where:

`--file <path to the configuration file>` is the full path to the configuration file to which you want to output the settings.

`--json`: output data in JSON format.

To edit Web Control settings, run the following command:

```
kesl-control --set-settings 26 [--file <path to the configuration file>] [--json]
```

where:

`--file <path to the configuration file>` is the full path to the configuration file from which you want to import the settings.

`--json` – import data from a JSON file.

To delete configured settings and reset Web Control settings to the default rule, run the following command:

```
kesl-control --set-settings 26 --set-to-default
```

Application Control

In the command line, you can manage Application Control by using the Application Control predefined task (`Application_Control`).

By default, the Application Control task does not run. You can start and stop the task manually.

You can configure Application Control on a device by editing the settings of the Application Control predefined task.

If you change the list of allowed applications or prohibit the launch of all applications or applications affecting Kaspersky Endpoint Security's operation, then when modifying the task settings using the configuration file or using command line options, run the following command:

```
kesl-control --set-settings --accept
```

You can also configure Application Control using Application Control commands:

- Create and edit lists of categories.
- View the list of categories created in the application.
- Configure the list of application control rules.

Application Control task

The table describes all possible values and the default values of all the settings that you can specify for the Application Control task (`Application_Control`).

Application Control task settings

Setting	Description	Values
`AppControlMode`	Application Control task operation mode.	`AllowList` – Kaspersky Endpoint Security prevents users from launching any applications that are not specified in the Application Control rules. `DenyList` (default value) – Kaspersky Endpoint Security allows users to launch any applications that are not specified in the Application Control rules.
`AppControlRulesAction`	The action that Kaspersky Endpoint Security performs upon detecting an attempt to start an application that matches the configured rules.	`ApplyRules` (default value) – Kaspersky Endpoint Security applies Application Control rules and performs the action specified in the rules. `TestRules` – Kaspersky Endpoint Security tests the rules and generates an event about the detection of an application that satisfies the rule.
The **[Categories.item_#]** section contains the following settings:		
`Name`	Name of the application category to which the rule applies.	
`UseIncludes`	Usage of inclusive conditions to trigger the rule.	`Yes` – apply the rule to the application if the application meets at least one inclusive condition. `No` (default value) – do not apply the rule to the application, even if the application meets the inclusive conditions.
`IncludeFileNames.item_#`	Name of the executable file that triggers the rule.	You can use masks to specify the file name.
`IncludeFolders.item_#`	Name of the directory with the application's executable file that triggers the rule.	You can use masks to specify the directory name.
`IncludeHashes.item_#`	SHA256 hash of the executable file that triggers the rule.	Only SHA256 can be used.
`UseExcludes`	Usage of excluding conditions to trigger the rule.	`Yes` – do not apply the rule to the application if the application meets at least one exclusive condition or does not meet any of the inclusive conditions. `No` (default value) – apply the rule to the application, even if the application meets at least one exclusive condition.
`ExcludeFileNames.item_#`	Name of the executable file that triggers the rule.	You can use masks to specify the file name.
`ExcludeFolders.item_#`	Name of the directory with the application's executable file that triggers the rule.	You can use masks to specify the directory name.

Setting	Description	Values
`ExcludeHashes.item_#`	SHA256 hash of the executable file that triggers the rule.	Only SHA256 can be used.
The **[AllowListRules.item_#]** section contains a list of Application Control rules for the *AllowList* operation mode. Each [AllowListRules.item_#] section contains the following settings:		
`Description`	Description of the Application Control rule.	
`AppControlRuleStatus`	Operation status of the Application Control rule:	`On` (default value): the rule is enabled, Kaspersky Endpoint Security applies this rule for the Application Control. `Off`: the rule is not used for the Application Control. `Test` – Kaspersky Endpoint Security allows applications covered by the rule to be launched, but logs information about the launch of these applications in the report.
`Category`	Name of the application category for which the rule applies. You can specify the "Golden Image" category.	
The **[AllowListRules.item_#.ACL.item_#]** section contains a list of users who are allowed or denied to run applications.		
`Access`	Access type assigned to a user or user group.	`Allow` (default value) — Allow running applications. `Block` – Deny running applications.
`Principal`	User or user group to which the Application Control rule applies.	`\Everyone` (default value): the rule applies to all users. `< user name >` is the name of the user to which the rule applies. `@< group name >` is the name of the group of users to which the rule applies.
The **[DenyListRules.item_#]** section contains a list of Application Control rules for the *DenyList* operation mode. Each [DenyListRules.item_#] section contains the following settings:		
`Description`	Description of the Application Control rule.	
`AppControlRuleStatus`	Operation status of the Application Control rule:	`On` (default value): the rule is enabled, Kaspersky Endpoint Security applies this rule for the Application Control. `Off`: the rule is not used for the Application Control. `Test` – Kaspersky Endpoint Security allows applications covered by the rule to be launched, but logs information about the launch of these applications in the report.
`Category`	Name of the created application category to which the rule applies. You can specify the "Golden Image" list of applications as a category.	
The **[DenyListRules.item_#.ACL.item_#]** section contains a list of users who are allowed or denied to run applications.		
`Access`	Access type assigned to a user or user group.	`Allow` – allow applications to start. `Block` (default value) – do not allow applications to start.
`Principal`	User or user group to which the Application Control rule applies.	`\Everyone` (default value): the rule applies to all users. `< user name >` is the name of the user to which the rule applies. `@< group name >` is the name of the group of users to which the rule applies.

Useful articles

How to specify masks

You can use the * character (any sequence of characters) or the ? character (any one character) as the file or directory name mask.

You can put the * character to represent any set of characters (including an empty set) in a file or directory name that includes the / character. For example, `/dir/*/file*/` or `/dir/file*/`.

You can put a single ? character to represent any one character (including `/`) in the file or directory name.

Creating and editing a list of categories

You can create a new category in two ways:

- using the "kesl --set-settings" command and the Application Control task settings configuration file (`Application_Control`).
- using the kesl --set-categories command and the category settings configuration file.

To create application categories, run the following command:

```
kesl-control --set-categories --file <path to the configuration file>
```

where:

`--file <path to the configuration file>` is the path to the configuration file with category settings.

The file with category settings must have the following structure:

```
[
   {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 1>"
   },
 {
      "Exclude" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "GUID" : "<unique category identifier>",
      "Include" : [ "(FilePath like <full path to the application's executable file>)", "(FileHash == <hash of the executable file>)" ],
      "Name" : "<category name 2>"
   }
]
```

To specify the file name in the `Exclude` and `Include` fields, you can use masks.

> The `Name` setting is required. If you do not specify the name of the category, it will not be created or will be deleted. The `GUID` setting is also required. If you do not specify it, an error message is displayed and the category is not created. The `GUID` setting must be specified without hyphens.

To edit the list of created application categories, run the following command:

```
kesl-control --set-categories [--names <category name 1> <category name 2> ... <category name N>] --file <path to the configuration file>
```

where:

- `<category name 1> <category name 2> ... <category name N>` are the names of the categories for which you want to edit information. If you want to change information about several categories, specify the names of the categories, separated by a space. If you do not specify a category name, existing categories are deleted and new categories are created from the specified file.
- `--file <path to the configuration file>` is the path to the configuration file with category settings.

Useful articles

How to specify masks

You can use the * character (any sequence of characters) or the ? character (any one character) as the file or directory name mask.

You can put the * character to represent any set of characters (including an empty set) in a file or directory name that includes the / character. For example, `/dir/*/file*/` or `/dir/file*/`.

You can put a single ? character to represent any one character (including `/`) in the file or directory name.

Viewing the list of categories

On the command line, you can view the list of created application categories using the Application Control command, `kesl-control --get-categories`.

The list of created categories contains the following categories:

- Categories created in Kaspersky Security Center.
- Categories added in the Application Control task settings using the command line.
- The "GoldenImage" category created using the Inventory task (in Kaspersky Security Center or using the command line).

To view the list of all created application categories, run the following command:

```
kesl-control --get-categories [--file <path to the configuration file>] [--json]
```

where:

- `--file <path to the configuration file>` is the full path to the configuration file to which you want to output the settings.
- `--json` is specified to output the settings in JSON format.

Kaspersky Endpoint Security displays the following information about the each application category:

- Unique identifier (GUID) of the category
- Category name

- list of inclusive conditions to trigger the rule
- list of exclusive conditions to trigger the rule

To view the list of separate application categories, execute the following command:

```
kesl-control --get-categories [--names <category name 1> <category name 2> ... <category name N>] [--file <path to the configuration file>] [--json]
```

where:

- `<category name 1> <category name 2> ... <category name N>` are the names of the categories for which you want to view information. If you want to view information about several categories, specify the names of the categories, separated by a space.
- `--file <path to the configuration file>` – full path to the JSON configuration file to which the category list will be exported.
- `--json` is specified to output the settings in JSON format.

If in the Application Control task settings, in the `[Categories.item_#]` section for inclusive or exclusive conditions for triggering a rule, you specify symbolic links to an application file or directory with executable files, then when viewing the list of categories for these conditions, the source path to which the symbolic link points is displayed.

Configuring the Application Control rule list

To view the list of Application Control rules, run the following command:

```
kesl-control --get-settings 21 [--file <path to the configuration file>] [--json]
```

where:

- `--file <path to the configuration file>` is the full path to the configuration file to which you want to output the settings.
- `--json`: output data in JSON format.

Kaspersky Endpoint Security displays the following information about Application Control rules:

- Application Control task operation mode.
- Action that Application Control takes upon detecting an attempt to launch an application that matches the configured rule.
- Description of the Application Control rule (if any).
- Operation status of the Application Control rule.
- Name of the application category the rule applies to.

- Access type assigned to a user or user group.
- Uuser or user group to which the Application Control rule applies.

To edit the list of application categories and Application Control rules, run the following command:

```
kesl-control --set-settings 21 [--file <path to the configuration file>] [--json]
```

where:

- `--file <path to the configuration file>` is the full path to the configuration file from which you want to import the settings.
- `--json` – import data from a JSON file.

To delete the list of application categories and Application Control rules, run the following command:

```
kesl-control --set-settings 21 --set-to-default
```

Configuring Inventory

You can use the command line to inventory applications on the protected device as follows:

- With the help of the Inventory predefined task (`Inventory_Scan`). You can manually start or stop this task, and configure the task schedule. You can configure scan settings by editing the settings of this task.
- With the help of user inventory tasks (tasks of the `InventoryScan` type). You can manually start, stop, pause, or resume user tasks and configure the task schedule.

You can view the list of applications detected on the device as a result of the Inventory task by using Application Control management commands.

Inventory task

The table describes all possible values and the default values of all the settings that you can specify for the Inventory task (`Inventory_Scan`).

Inventory task settings

Setting	Description	Values
`ScanScripts`	Enables script scanning.	`Yes` (default value) — Scan scripts. `No` — Do not scan scripts.
`ScanBinaries`	Enables binary files scanning (elf, java, and pyc).	`Yes` (default value) — Scan binaries. `No` — Do not scan binaries.
`ScanAllExecutable`	Enables the scanning of files with an executable bit.	`Yes` (default value) — Scan files with an executable bit. `No` — Do not scan files with an executable bit.

Setting	Description	Values
`GoldenImageAction`	The action that Kaspersky Endpoint Security must perform with the Golden Image application category upon completion of the Inventory task: You can use the "Golden Image" category in Application Control rules.	`DoNothing` (default) – do not change the Golden Image application category after completing the inventory. `Create` – add detected applications to the Golden Image application category. If the category does not exist, it is created. If the category exists, the list of applications in the category is updated. `Remove` – clear the Golden Image application category. The category is cleared immediately the task is started, without doing an inventory of files on the device.
The **[ScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the inventory scope. The maximum length of the string specified using this setting is 4096 characters.	Default value: `All objects`.
`UseScanArea`	Enables scans of the specified inventory scope. To run the task, enable scans of at least one inventory scope.	`Yes` (default value) — Scan the specified inventory scope. `No` — Do not scan the specified inventory scope.
`AreaMask.item_#`	Inventory scan scope limitation. In the inventory scan scope, the application scans only the files that are specified using the masks in the shell format. If this setting is not specified, the application scans all the objects in the inventory scope. You can specify several values for this setting.	The default value is `*` (scan all objects).
`Path`	Path to the directory with objects to be scanned.	`< path to local directory >` — scan objects in the specified directory. Default value: `/usr/bin`
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the inventory exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from the inventory.	`Yes` (default value) — Exclude the specified scope. `No` — Do not exclude the specified scope.
`AreaMask.item_#`	Limiting the inventory exclusion scope using shell masks. If this setting is not specified, the application excludes all the objects in the inventory scope. You can specify several values for this setting.	Default value: `*` (exclude all objects)
`Path`	Path to the directory with objects to be excluded.	`< path to local directory >` excludes objects in the specified directory from the scan. You can use masks to specify the path.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Viewing a list of detected applications

To view the list of applications detected on the device, execute the following command:

```
kesl-control --get-app-list [--json]
```

where `--json` means output data in JSON format.

Kaspersky Endpoint Security displays the following information about the detected applications:

- **Date and time of inventory**. Date and time when the Inventory task was performed
- **Number of applications**. The number of applications detected on the device
- The list of applications containing the following information:
  - **Path**. Path to the application.
  - **Hash**. Application hash sum.
  - **Type**. Application type. For example, `Script`, `Executable`.
  - **Categories**. Categories that the application belongs to (if they were previously created). You can view the list of created application categories using the following command:

    ```
    kesl-control --get-categories
    ```

> When you add a new category, its information is not automatically updated in the application list. To update the application list, you need to restart the Inventory task.

System Integrity Monitoring task

You can manage system integrity monitoring in real time in the command line by using the System Integrity Monitoring predefined task (`System_Integrity_Monitoring`). The `OAFIM` task type.

The System Integrity Monitoring task does not run by default. You can start and stop the task manually.

You can configure System Integrity Monitoring on the device by editing the settings of the System Integrity Monitoring predefined task.

Setting	Description	Values
`UseExcludeMasks`	Enables monitoring scope exclusions for objects specified by the `ExcludeThreats.item_#` setting. This setting applies only if the `ExcludeMasks.item_#` setting is specified.	`Yes` — Exclude the objects specified by the `ExcludeMasks.item_#` setting from the monitoring scope. `No` (default value) — Do not exclude the objects specified by the `ExcludeMasks.item_#` setting from the monitoring scope.
`ExcludeMasks.item_#`	Excludes objects from monitoring by names or masks. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format. Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled. You can specify several masks. Each mask must be specified on a new line with a new index.	The default value is not defined.
The [ScanScope.item_#] section contains the monitoring scopes of the System Integrity Monitoring task. At least one monitoring scope must be specified for the task. You can specify several [ScanScope.item_#] sections in any order. The application processes the scopes by index in ascending order. The [ScanScope.item_#] section contains the following settings:		
`AreaDesc`	Description of monitoring scope; contains additional information about the monitoring scope.	The default value is not defined.
`UseScanArea`	Enables monitoring of the specified scope.	`Yes` (default value) — Monitor the specified scope. `No` — Do not monitor the specified scope.
`Path`	Path to the monitoring directory.	You can use masks to specify the path. Default value: /opt/kaspersky/kesl/
`AreaMask.item_#`	Monitoring scope limitation. Within the monitoring scope, the application scans only the objects that are specified using the masks in the shell format. You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	Default value: `*` (all objects are monitored)
[ExcludedFromScanScope.item_#] contains objects to be excluded from all [ScanScope.item_#] sections. You can specify multiple [ExcludedFromScanScope.item_#] sections in any order. The application processes the scopes by index in ascending order. The [ExcludedFromScanScope.item_#] section contains the following settings:		
`AreaDesc`	Description of the monitoring exclusion scope, which contains additional information about the monitoring exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from monitoring.	`Yes` (default value) — Exclude the specified scope from monitoring. `No` — Do not exclude the specified scope from monitoring.
`Path`	Path to the directory with objects excluded from monitoring.	You can use masks to specify the path. The default value is not defined.
`AreaMask.item_#`	Limitation of monitoring exclusion scope. In the monitoring exclusion scope, the application only excludes the objects that are specified using masks in the shell format. You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	Default value: `*` (exclude all objects from monitoring).

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

System Integrity Check task

You can run a system integrity check on a device in the command line by using custom System Integrity Check tasks (`System_Integrity_Monitoring`). The `ODFIM` task type.

You can manually start, stop, pause, or resume user tasks and configure the task schedule. You can configure system integrity checking by editing the settings of these tasks.

System Integrity Check task settings

Setting	Description	Values
`RebuildBaseline`	Enables baseline to rebuild after the *System Integrity Check* task finishes.	`Yes`: rebuild the baseline every time the *System Integrity Check* task finishes. `No` (default): do not rebuild the baseline every time the *System Integrity Check* task finishes.
`CheckFileHash`	Use the file hash (SHA256) as a criterion when comparing the current state of the monitored file with its original state.	`Yes`: check the hash. `No` (default value) — Disable hash check. If this check is disabled, the application compares only the file size (if the file size has not changed, then the modification time is not considered a critical parameter).
`TrackDirectoryChanges`	Enables directory monitoring.	`Yes`: monitor directories while checking system integrity. `No` (default value) — Do not monitor directories.
`TrackLastAccessTime`	Enables tracking last file access time. In the Linux operating systems it is the `noatime` setting.	`Yes` — Track last file access time. `No` (default value) — Do not track last file access time.
`UseExcludeMasks`	Enables monitoring scope exclusions for objects specified by the `ExcludeMasks.item_#` setting. This setting applies only if the `ExcludeMasks.item_#` setting is specified.	`Yes` — Exclude the objects specified by the `ExcludeMasks.item_#` setting from the monitoring scope. `No` (default value) — Do not exclude the objects specified by the `ExcludeMasks.item_#` setting from the monitoring scope.
`ExcludeMasks.item_#`	Excludes objects from monitoring by names or masks. You can use this setting to exclude an individual file from the specified scan scope by name or exclude several files at once using masks in the shell format. Before specifying a value for this setting, make sure that the `UseExcludeMasks` setting is enabled. You can specify several masks. Each mask must be specified on a new line with a new index.	The default value is not defined.
The [ScanScope.item_#] section contains the monitoring scopes of the *System Integrity Check*. At least one monitoring scope must be specified for the task. You can specify several [ScanScope.item_#] sections in any order. The application processes the scopes by index in ascending order. The [ScanScope.item_#] section contains the following settings:		
`AreaDesc`	Description of monitoring scope; contains additional information about the monitoring scope.	The default value is not defined.
`UseScanArea`	Enables monitoring of the specified scope.	`Yes` (default value) — Monitor the specified scope. `No` — Do not monitor the specified scope.

Setting	Description	Values
`Path`	Path to the monitoring directory.	You can use masks to specify the path. Default value: /opt/kaspersky/kesl/
`AreaMask.item_#`	Monitoring scope limitation. Within the monitoring scope, the application scans only the objects that are specified using the masks in the shell format. You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	Default value: `*` (all objects are monitored)
The **[ExcludedFromScanScope.item_#]** section contains the objects to be excluded from all [ScanScope.item_#] sections. You can specify several [ExcludedFromScanScope.item_#] sections in any order. The application processes the scopes by index in ascending order. The [ExcludedFromScanScope.item_#] section contains the following settings:		
`AreaDesc`	Description of the monitoring exclusion scope, which contains additional information about the monitoring exclusion scope.	The default value is not defined.
`UseScanArea`	Excludes the specified scope from monitoring.	`Yes` (default value) — Exclude the specified scope from monitoring. `No` — Do not exclude the specified scope from monitoring.
`Path`	Path to the directory with objects excluded from monitoring.	You can use masks to specify the path. The default value is not defined.
`AreaMask.item_#`	Limitation of monitoring exclusion scope. In the monitoring exclusion scope, the application only excludes the objects that are specified using masks in the shell format. You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	Default value: `*` (exclude all objects from monitoring).

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Protection against advanced threats and targeted attacks

Kaspersky Endpoint Detection and Response Expert (on-premises) Integration

You can manage the integration between Kaspersky Endpoint Security and the Kaspersky Endpoint Detection and Response Expert (on-premises) solution via the *Kaspersky Endpoint Detection and Response Expert (on-premises) (KATAEDR)* predefined task on the command line.

> This task also allows you to manage the Kaspersky Endpoint Detection and Response (KATA) Integration settings. For the Kaspersky Endpoint Detection and Response Expert (on-premises) integration, you need to select the *EDR Expert (on-premises)* integration mode and manage the integration settings as necessary.

You can manage Kaspersky Endpoint Detection and Response Expert (on-premises) Integration settings by editing the settings of the predefined task.

The *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task does not run by default. You can start and stop the task manually.

You can manage the certificates used for connecting to OSMP servers using the EDR Expert (on-premises) component management commands.

Kaspersky Endpoint Detection and Response Expert (on-premises) Integration settings

The table below describes the settings of the Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`) Integration predefined task, which you can manage when integrating with Kaspersky Endpoint Detection and Response Expert (on-premises).

> This task also allows you to manage the Kaspersky Endpoint Detection and Response (KATA) Integration settings. For the Kaspersky Endpoint Detection and Response Expert (on-premises) integration, you need to select the *EDR Expert (on-premises)* integration mode (`Mode=EDRExpertOnPrem`) in the task settings.

Kaspersky Endpoint Detection and Response Expert (on-premises) Integration settings

Setting	Description	Value
`Mode`	Integration mode. For the Kaspersky Endpoint Detection and Response Expert (on-premises) integration, the Kaspersky Endpoint Security application interacts with servers on the OSMP platform. For the Kaspersky Endpoint Detection and Response (KATA) integration, the Kaspersky Endpoint Security application interacts with servers on the Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (default) is the EDR (KATA) integration mode. Allows enabling integration with Kaspersky Endpoint Detection and Response (KATA), a component of Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` is the EDR Expert (on-premises) integration mode. Enables the Kaspersky Endpoint Detection and Response Expert (on-premises) integration
`UseClientPinnedCertificate`	Enable or disable two-way authentication for additional security of the connection to the OSMP threat response action server. If two-way authentication is enabled on the OSMP threat response server side, you need to enable two-way authentication in the settings of *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task and add the client certificate before starting the task.	`Yes` enables two-way authentication for additional security of the connection to the OSMP threat response action server. `No` (default value) — do not use two-way authentication.

Setting	Description	Value
`SynchronizationPeriod`	Periodicity of synchronization requests to the OSMP threat response action server, in minutes.	Default value: `5`.
`ConnectionTimeout`	The maximum time to wait for a connection to the OSMP threat response action server, in seconds.	Default value: `10`.
`RequestTimeout`	The maximum time to wait for a response from the OSMP threat response action server, in seconds.	Default value: `10`.
`EnableTelemetry`	Sending data about events on devices (telemetry) to the OSMP telemetry collection server.	`Yes` (default value) enables the sending of telemetry to the OSMP telemetry server. `No` disables the sending of telemetry.
The **[Endpoints.item_#]** section contains the address and port of the OSMP threat response action server. You can add multiple servers.		
`Address`	OSMP threat response action server address. IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port for connecting to the OSMP threat response server.	Default value: `443`.
The **[TelemetrySettings]** section contains general settings for connecting to OSMP telemetry servers.		
`UseClientPinnedCertificate`	Enable or disable two-way authentication for additional security of the connection to the OSMP telemetry server. If two-way authentication is enabled on the OSMP telemetry server side, you need to enable two-way authentication in the settings of *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task and add the client certificate before starting the task.	`Yes` enables two-way authentication for additional security of the connection to the OSMP telemetry server. `No` (default value) — do not use two-way authentication.
`ConnectionTimeout`	The maximum time to wait for a connection to the OSMP telemetry server, in seconds.	Default value: `10`.
`RequestTimeout`	The maximum time to wait for a response from the OSMP telemetry server, in seconds.	Default value: `10`.
`OnlyTaggedEvents`	Sending telemetry with IOA only. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the *streaming scan* technology, which allows real time tracking of such events.	`Yes` – send only telemetry with an Indicator of Attack (IOA). `No` (default) – send all telemetry.
The **[TelemetrySettings.Endpoints.item_#]** section contains the address and port of the OSMP telemetry server. You can add multiple servers.		
`Address`	OSMP telemetry server certificate address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port for connecting to the OSMP telemetry server.	Default value: `443`.
The **[TelemetrySettings.EventTransferSettings]** section contains settings for data transfer to the OSMP telemetry server.		
`MaximumDataTransferTime`	The maximum delay in sending events to the OSMP telemetry server in seconds.	Default value: `30`.
`UseRequestCountLimits`	Limit the number of requests. This feature helps optimize the load on the server. If this functionality is enabled, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Endpoint Security stops sending events.	`Yes` (default value) – regulate the number of events sent. `No` – do not regulate the number of events.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	Default value: `3000`.

Setting	Description	Value
`MaximumNumberOfEventsInPackage`	Maximum number of events in one package.	Default value: `1024`.
`EventLimitExceededPercentage`	Number of events above the limit (percentage). Sending events is limited if the ratio of events of a certain type to the total number of events exceeds the configured threshold (as a percentage).	Default value: `15`.

Managing certificates for connecting to OSMP EDR Expert (on-premises) servers

Managing certificates requires the rights of a user with the Administrator (admin) role.

You can use commands to manage the certificates used for the connection to OSMP servers. You can do the following with certificates:

- Add or replace certificates of OSMP servers: the threat response server and the telemetry server
- Display information about server certificates
- Delete server certificates
- Add or replace client certificates used to protect the connection to OSMP servers: the threat response server and the telemetry server
- Display information about the client certificates
- Delete client certificates

Managing certificates for the connection to the OSMP threat response server

To add or replace the threat response action server certificate, run the following command:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type response
```

where `<file>` is the path to the file containing the server certificate.

To add or replace the client certificate for the threat response server connection:

1. Run the following command:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type response
   ```

   where `<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

2. Enter the crypto-container password

The client certificate is used for additional protection of the connection to the OSMP server if client certificate verification is enabled in OSMP server settings and in the *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task settings, the `UseClientPinnedCertificate` setting in the `[KATAEDR]` section has the value `yes`.

To display information about the threat response action server certificate, run the following command:

```
kesl-control [-R] --query-kataedr-server-certificate --server-type response
```

To display information about the client certificate used to secure the connection to the threat response action server, run the following command:

```
kesl-control [-R] --query-kataedr-client-certificate --server-type response
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

To delete the threat response action server certificate, run the following command:

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type response
```

To delete the client certificate used to secure the connection to the threat response action server, run the following command:

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type response
```

Managing certificates for connecting to the OSMP telemetry server

To add or replace the certificate of the telemetry server, run the following command:

```
kesl-control [-R] --add-kataedr-server-certificate <file> --server-type telemetry
```

where `<file>` is the path to the file containing the server certificate.

To add or replace the client certificate for the telemetry server connection:

1. Run the following command:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file> --server-type telemetry
   ```

   where `<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

2. If the cryptocontainer is password-protected, enter the password when prompted.

The client certificate is used for additional protection of the connection to the OSMP server if client certificate verification is enabled in OSMP server settings and in the *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task settings, the `UseClientPinnedCertificate` setting in the `[TelemetrySettings]` section has the value `yes`.

To display information about the telemetry server certificate, run the following command:

```
kesl-control [-R] --query-kataedr-server-certificate --server-type telemetry
```

To display information about the client certificate used to secure the connection to the telemetry server, run the following command:

```
kesl-control [-R] --query-kataedr-client-certificate --server-type telemetry
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

To delete the telemetry server certificate, run the following command:

```
kesl-control [-R] --remove-kataedr-server-certificate --server-type telemetry
```

To delete the client certificate used to secure the connection to the telemetry server, run the following command:

```
kesl-control [-R] --remove-kataedr-client-certificate --server-type telemetry
```

Kaspersky Endpoint Detection and Response Expert (cloud) integration

You can manage the integration between Kaspersky Endpoint Security and the Kaspersky Endpoint Detection and Response Expert (cloud) solution via the *Kaspersky Endpoint Detection and Response Expert (cloud) integration* predefined task on the command line.

You can manage Kaspersky Endpoint Detection and Response Expert (cloud) Integration settings by editing the settings of the predefined task.

The *Kaspersky Endpoint Detection and Response Expert (cloud) Integration* task does not run by default. You can start and stop the task manually.

Kaspersky Endpoint Detection and Response Expert (cloud) integration settings

The following table describes the settings of the Kaspersky Endpoint Detection and Response Expert (cloud) Integration predefined task (`EDRExpertCloud`).

```
How to get the current values of task settings

kesl-control --get-settings 39
```

```
How to configure task settings

kesl-control --set-settings 39 <parameter>=<value>
```

Kaspersky Endpoint Detection and Response Expert (cloud) integration settings

Setting	Description
Response server integration settings	
`UseTunnel`	Using a TCP tunnel for connecting to the response server. TCP tunnel is used for connecting to the server if the security policy in your infrastructure does not allow you to connect directly to servers. By default, using a TCP tunnel is disabled (`No`).
`TunnelAddress`	Server address (IPv4 or IPv6) for connecting to the tunnel.
`TunnelPort`	Server port for connecting to the tunnel.
`SynchronizationPeriod`	Periodicity of synchronization requests to the OSMP threat response action server, in minutes. Default value: `5`.
Telemetry collection server integration settings The `[TelemetrySettings]` section contains general settings for connecting to OSMP telemetry servers.	
`EnableTelemetry`	Sending data about events on devices (telemetry) to the OSMP telemetry collection server. Sending telemetry is enabled by default (`Yes`).
`OnlyTaggedEvents`	Sending telemetry with IOA only. *Indicator of Attack (IOA)* is a rule that contains a description of suspicious behavior in the system that may indicate a targeted attack. The application compares ongoing behavior in the system with these rules and logs events that are indicative of a targeted attack. The application uses the *streaming scan* technology, which allows real time tracking of such events. By default, sending telemetry with IOA only is disabled (`No`).
`UseTunnel`	Using a TCP tunnel for connecting to the telemetry collection server. TCP tunnel is used for connecting to the server if the security policy in your infrastructure does not allow you to connect directly to servers. By default, using a TCP tunnel is disabled (`No`).
`TunnelAddress`	Server address (IPv4 or IPv6) for connecting to the tunnel.
`TunnelPort`	Server port for connecting to the tunnel.

Setting	Description
The `[TelemetrySettings.EventTransferSettings]` section contains general settings for connecting to OSMP telemetry servers.	
`UseRequestCountLimits`	Limit the number of requests. This feature helps optimize the load on the server. If this functionality is enabled, the application restricts the transmitted events. If the number of events exceeds the configured limits, Kaspersky Endpoint Security stops sending events. This option is disabled by default.
`MaximumDataTransferTime`	Maximum delay when sending events. The application synchronizes with the server to send events after the synchronization interval expires. The default setting is 30 seconds.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour The application analyzes the telemetry data stream and restricts the sending of events if the event stream exceeds the configured events-per-hour limit. Kaspersky Endpoint Security resumes sending events after an hour. The default setting is 3000 events per hour. If the application is installed on a server, the telemetry data stream is higher. For servers, it is recommended to increase the value to 60,000 events per hour.
`MaximumNumberOfEventsInPackage`	Maximum number of events in a package. The application synchronizes with the server when the buffer is filled with events. The default setting is 1024 events.
`EventLimitExceededPercentage`	Event throttle threshold (percentage). The application sorts events by type (for example, "changes in the registry" events) and restricts transmission of events if the ratio of events of the same type to the total number of events exceeds the configured limit in percent. Kaspersky Endpoint Security resumes sending events when the ratio of other events to the total number of events becomes big enough again. The default setting is 15 %.

Managing OSMP EDR Expert servers (cloud) connection certificates

Managing certificates requires the rights of a user with the Administrator (admin) role.

The application receives server addresses and certificates for establishing a trusted connection automatically after you accept the terms and conditions of the Kaspersky Endpoint Detection and Response Expert (cloud) agreement on data processing. Therefore, you cannot add or remove certificates using commands. You can only display information about certificates on the command line.

Managing certificates for the connection to the OSMP threat response server

```
To display information about the threat response server certificate
```

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type response
```

```
To display information about the client certificate for the threat response server connection
```

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type response
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

Managing certificates for connecting to the OSMP telemetry server

```
Displaying information about the telemetry collection server certificate
```

```
kesl-control [-R] --query-cloudxdr-server-certificate --server-type telemetry
```

```
To display information about the client certificate for the telemetry server connection
```

```
kesl-control [-R] --query-cloudxdr-client-certificate --server-type telemetry
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

Kaspersky Endpoint Detection and Response (KATA) Integration

You can manage the integration between Kaspersky Endpoint Security and the Kaspersky Endpoint Detection and Response (KATA) component via the *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration (KATAEDR)* predefined task on the command line.

> This task also allows you to manage the Kaspersky Endpoint Detection and Response Expert (on-premises) integration settings. For the integration with Kaspersky Endpoint Detection and Response (KATA), you need to select the EDR (KATA) integration mode in the task settings and manage the integration settings as necessary.

You can configure Kaspersky Endpoint Detection and Response (KATA) Integration settings by editing the settings of the predefined task.

The *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task does not run by default. You can start and stop the task manually.

You can manage the certificates used for connecting to KATA servers using the EDR Expert (on-premises) component management commands.

Kaspersky Endpoint Detection and Response (KATA) integration settings

The table below describes the settings of the Kaspersky Endpoint Detection and Response Expert (on-premises) (`KATAEDR`) Integration predefined task, which you can manage when integrating with Kaspersky Endpoint Detection and Response (KATA).

> This task also allows you to manage the Kaspersky Endpoint Detection and Response Expert (on-premises) integration settings. For the integration with Kaspersky Endpoint Detection and Response (KATA), you need to select the *EDR (KATA)* integration mode in the task settings (`Mode=EDRKATA`).

Kaspersky Endpoint Detection and Response (KATA) integration settings

Setting	Description	Value
`Mode`	Integration mode. For the Kaspersky Endpoint Detection and Response Expert (on-premises) integration, the Kaspersky Endpoint Security application interacts with servers on the OSMP platform. For the Kaspersky Endpoint Detection and Response (KATA) integration, the Kaspersky Endpoint Security application interacts with servers on the Kaspersky Anti Targeted Attack Platform.	`EDRKATA` (default) is the EDR (KATA) integration mode. Allows enabling integration with Kaspersky Endpoint Detection and Response (KATA), a component of Kaspersky Anti Targeted Attack Platform. `EDRExpertOnPrem` is the EDR Expert (on-premises) integration mode. Enables the Kaspersky Endpoint Detection and Response Expert (on-premises) integration
`UseClientPinnedCertificate`	Enable and disable two-way authentication to further secure the connection to the KATA server. If two-way authentication is enabled on the KATA server side, you need to enable two-way authentication in the settings of *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task and add the client certificate before starting the task.	`Yes` – use two-way authentication to further secure the connection to the KATA server. `No` (default value) — do not use two-way authentication.
`SynchronizationPeriod`	Frequency of sending synchronization requests to the KATA server in minutes.	Default value: `5`.
`ConnectionTimeout`	Maximum time to wait for a connection to the KATA server in seconds.	Default value: `10`.
`RequestTimeout`	Maximum time to wait for a response from the KATA server in seconds.	Default value: `10`.
`EnableTelemetry`	Sending event data (telemetry) to KATA.	`Yes` (default value) – send telemetry to the KATA server. `No` disables the sending of telemetry.
The **[Endpoints.item_#]** section contains the address and port of the KATA server. You can add multiple servers.		
`Address`	KATA server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port to connect to the KATA server.	Default value: `443`.
The **[EventTransferSettings]** section contains settings for sending data to the KATA server.		
`MaximumDataTransferTime`	The maximum delay in sending events to the KATA server in seconds.	Default value: `30`.
`UseRequestCountLimits`	Enable and disable regulating the number of events sent to the KATA server.	`Yes` (default value) – regulate the number of events sent. `No` – do not regulate the number of events.

Setting	Description	Value
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	Default value: `3000`.
`MaximumNumberOfEventsInPackage`	Maximum number of events in one package.	Default value: `1024`.
`EventLimitExceededPercentage`	Number of events above the limit (percentage). Sending events is limited if the ratio of events of a certain type to the total number of events exceeds the configured threshold (as a percentage).	Default value: `15`.

Managing certificates for connecting to the KATA server

Managing certificates requires the rights of a user with the Administrator (admin) role.

You can use commands to manage the certificates used for the connection to the KATA server. You can do the following with certificates:

- Add or replace the KATA server certificate
- Display information about the server certificate
- Remove the server certificate
- Delete or replace the client certificate used to secure the connection to a KATA server
- Display information about the client certificate
- Remove the client certificate

To add or replace the server certificate, run the following command:

```
kesl-control [-R] --add-kataedr-server-certificate <file>
```

where `<file>` is the path to the file containing the server certificate.

To add or change a client certificate:

1. Run the following command:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file>
   ```

   where `<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

2. Enter the crypto-container password

The client certificate is used for additional protection of the connection to the KATA server if client certificate verification is enabled in KATA server settings and in the *Kaspersky Endpoint Detection and Response Expert (on-premises) Integration* task settings, `UseClientPinnedCertificate` is set to `yes`.

To display the server certificate information, run the following command:

```
kesl-control [-R] --query-kataedr-server-certificate
```

To display the client certificate information, run the following command:

```
kesl-control [-R] --query-kataedr-client-certificate
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

To delete the server certificate information, run the following command:

```
kesl-control [-R] --remove-kataedr-server-certificate
```

To delete the client certificate information, run the following command:

```
kesl-control [-R] --remove-kataedr-client-certificate
```

Kaspersky Network Detection and Response (KATA) Integration

You can manage the integration between Kaspersky Network Security and Kaspersky Endpoint Detection and Response (KATA) via the *Kaspersky Network Detection and Response (KATA) Integration (`KATANDR`)* predefined task on the command line:

The *Kaspersky Network Detection and Response (KATA) Integration* does not run by default. You can start and stop the task manually.

You can configure Kaspersky Network Detection and Response (KATA) Integration settings by editing the settings of the predefined task.

You can manage the certificates used for connecting to NDR servers using the NDR (KATA) component management commands.

Kaspersky Network Detection and Response (KATA) integration settings

The table describes all available settings and the default values of all the settings that you can specify for the Kaspersky Network Detection and Response (KATA) Integration task (`KATANDR`).

Setting	Description	Value
`UseClientPinnedCertificate`	Enable and disable two-way authentication to further secure the connection to the NDR server. If client certificate validation is enabled on the NDR server side, enable the use of a client certificate and add a client certificate before starting the *Kaspersky Network Detection and Response (KATA) Integration* task.	`Yes` – use two-way authentication to further secure the connection to the NDR server. `No` (default value) — do not use two-way authentication.
`SynchronizationPeriod`	Frequency of sending synchronization requests to the NDR server in minutes.	Default value: `5`.
`ConnectionTimeout`	Maximum time to wait for a connection to the NDR server in seconds.	Default value: `10`.
`RequestTimeout`	Maximum time to wait for a response from the NDR server in seconds.	Default value: `10`.
The **[Endpoints.item_#]** section contains the address and port of the NDR server.		
`Address`	NDR server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified.	Default value: `127.0.0.1`.
`Port`	Port to connect to the NDR server.	Default value: `8081`.
The **[EventTransferSettings]** section contains settings for sending events to the NDR server.		
`MaximumDataTransferTime`	The maximum delay in sending events to the NDR server in seconds.	Default value: `30`.
`MaximumNumberOfEventsInPackage`	Maximum number of events in one package.	Default value: `1024`.
`UseRequestCountLimits`	Enable and disable regulating the number of events sent to the NDR server.	`Yes` (default value) – regulate the number of events sent. `No` – do not regulate the number of events.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	Default value: `3000`.
`EventLimitExceededPercentage`	Event throttle threshold (percentage). Sending events is limited if the ratio of events of a certain type to the total number of events exceeds the configured threshold (as a percentage).	Default value: `15`.
`PingPeriod`	NDR server polling period in seconds.	Default value: `450`.

Managing certificates for connecting to the NDR server

Managing certificates requires the rights of a user with the Administrator (admin) role.

You can use commands to manage the certificates used for the connection to the NDR server. You can do the following with certificates:

- Add or replace the NDR server certificate
- Display information about the server certificate
- Remove the server certificate
- Delete or replace the client certificate used to secure the connection to an NDR server
- Display information about the client certificate
- Remove the client certificate

To add or replace the server certificate, run the following command:

```
kesl-control [-R] --add-katandr-server-certificate <file>
```

where `<file>` is the path to the file containing the server certificate.

To add or change a client certificate:

1. Run the following command:

   ```
   kesl-control [-R] --add-katandr-client-certificate <file>
   ```

   where `<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

2. Enter the crypto-container password

The client certificate is used for additional protection of the connection to the NDR server if client certificate verification is enabled in the NDR server settings and in the *Kaspersky Network Detection and Response (KATA) Integration* task settings, the `UseClientPinnedCertificate` setting is set to `yes`.

To display the server certificate information, run the following command:

```
kesl-control [-R] --query-katandr-server-certificate
```

To display the client certificate information, run the following command:

```
kesl-control [-R] --query-katandr-client-certificate
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

To delete the server certificate information, run the following command:

```
kesl-control [-R] --remove-katandr-server-certificate
```

To delete the client certificate information, run the following command:

```
kesl-control [-R] --remove-katandr-client-certificate
```

Sandbox Integration

On the command line, you can manage the integration of the Kaspersky Endpoint Security application with Sandbox using the *Sandbox Integration* predefined task.

By default, the *Sandbox Integration* task is not running. You can start and stop this task manually.

To start the Sandbox Integration task, execute the following command:

```
kesl-control --start-task 29
```

The *Integration with Sandbox* task cannot be started if the server certificate has not been added.

If the *Sandbox Integration* task has started and its selected mode allows sending files for scanning manually (`Manual` or `AutoAndManual`), you can send files to be scanned in Sandbox from the command line.

How to send files for scanning to Sandbox

```
kesl-control [-X] --sandbox <path>
```

where `<path>` is the path to the file or directory that you want to scan. You can specify multiple paths by separating them with a space.

You can manage the Sandbox integration settings by editing the settings for the predefined task.

Using the commands for managing the Sandbox integration settings, you can manage certificates that are used for connecting to servers responsible for interaction with Sandbox servers.

Sandbox integration settings

The table below describes all available settings and the default values of all the settings that you can specify for the Sandbox Integration task (`Standalone_Sandbox`).

How to configure Sandbox integration settings

```
kesl-control --set-settings 29 Servers.item_0000.Address=<server> Servers.item_0000.Port=<port> [<setting name>=
<setting value>]
```

Setting	Description	Value
`UseClientCertificate`	Enable and disable two-way authentication to further secure the connection to the Sandbox server. If client certificate validation is enabled on the Sandbox server side, enable the use of a client certificate and add a client certificate before starting the *Sandbox Integration* task.	`Yes` — use two-way authentication to further secure the connection to the Sandbox server. `No` (default value) — do not use two-way authentication.
`ConnectionTimeout`	Maximum time to wait for a connection to the server in seconds.	Default value: `10`.
`RequestTimeout`	Maximum time to wait for a response from the server in seconds.	Default value: `10`.
`SendingMode`	Mode of sending an object to Sandbox to be scanned	`AutoOnly` (default value) – automatically send files for scanning when an attempt is made to gain access to a file. `Manual` – send files for scanning manually. `AutoAndManual` – send files for scanning automatically as well as manually.
`QuarantineFile`	Quarantine file when a threat is detected.	`Yes` (default value) – if a threat is detected, delete the original file, place a copy of the file in Quarantine. `No` – do not quarantine the file when a threat is detected.
`ScanCriticalAreas`	Perform a critical areas scan when a threat is detected.	`Yes` (default value) – start a critical areas scan when a threat is detected. `No` – do not start a critical areas scan when a threat is detected.
`CreateIocScanTask`	Create an IOC Scan task when a threat is detected.	`Yes` (default) – create an IOC Scan task when a threat is detected. `No` – do not create an IOC Scan task when a threat is detected.
`QuarantineFileOnIocDetected`	Quarantine the object when an indicator of compromise is detected.	`Yes` (default value) – if an indicator of compromise is detected, delete the original object, place a copy of the object in Quarantine. `No` – do not quarantine the object when an indicator of compromise is detected.
`ScanCriticalAreasOnIocDetected`	Perform a critical areas scan when an indicator of compromise is detected.	`Yes` (default value) – start a critical areas scan when an indicator of compromise is detected. `No` – do not start a critical areas scan when an indicator of compromise is detected.
`Drives`	Scopes for the IoC scan.	`Critical` (default) – scan files in user and system directories. `System` – scan all files within the root file system.
`ScheduleMode`	IOC Scan task start mode.	`Manually` (default) – start the IOC Scan task manually. `AfterTreatDetected` – start the IOC Scan task after a threat is detected.
The **[Servers.item_#]** section contains the settings of the Sandbox server.		
`Address`	Address of the server. IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified.	Default value: `127.0.0.1`.
`Port`	Port for connecting to the server.	Default value: `443`.

Setting	Description	Value
The **[SandboxTransferSettings]** section contains settings for sending files for scanning in Sandbox.		
`SandboxQueue`	The maximum size of the scan request queue in megabytes.	Default value: `1024`.

Managing certificates for connecting to the Sandbox server

Managing certificates requires the rights of a user with the Administrator (admin) role.

You can manage the certificates used for the connections to OSMP servers or Central Node servers responsible for interaction with Sandbox (hereinafter also referred to as Sandbox servers) using commands. You can do the following with certificates:

- Add or replace the server certificate
- Display information about the server certificate
- Remove the server certificate
- Add or replace the client certificate
- Display information about the client certificate
- Remove the client certificate

To add or replace the server certificate, run the following command:

```
kesl-control [-X] --add-sandbox-server-certificate <file>
```

where `<file>` is the path to the file containing the server certificate.

To add or change a client certificate:

1. Run the following command:

   ```
   kesl-control [-X] --add-sandbox-client-certificate <file>
   ```

   where `<file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

2. Enter the crypto-container password

The client certificate is used for additional protection of the connection to the Sandbox server if client certificate verification is enabled in the Sandbox server settings and if in the settings of the *Sandbox Integration* task, `UseClientCertificate` is set to `yes`.

To display certificate information, run the following command:

- for the server certificate:

```
kesl-control [-X] --query-sandbox-server-certificate
```

- for the client certificate:

```
kesl-control [-X] --query-sandbox-client-certificate
```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

To delete the server certificate information, run the following command:

```
kesl-control [-X] --remove-sandbox-server-certificate
```

To delete the client certificate information, run the following command:

```
kesl-control [-X] --remove-sandbox-client-certificate
```

Enabling or disabling Kaspersky Endpoint Detection and Response Optimum integration

You can enable or disable the EDR Optimum component by using the `UseEdrOptimum` setting in the general application settings.

You can change the value of the setting with the help of command line switches or a configuration file that contains all general application settings.

To enable the EDR Optimum component using command line options:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

To disable the EDR Optimum component using command line options:

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Configuring the Kaspersky Managed Detection and Response integration

In the command line, you can do the following:

- Enable or disable the MDR component.
- Upload or delete the MDR BLOB file, which contains Kaspersky Managed Detection and Response license information.

  If the MDR component is activated with a license key, you do not need to upload the MDR BLOB file.

We recommend configuring the integration between Kaspersky Endpoint Security and Kaspersky Managed Detection and Response in the Administration Console or in the Web Console.

You can enable or disable the MDR component by editing the `UseMDR` option in the general application settings. You can change the value of the setting with the help of command line switches or a configuration file that contains all general application settings.

The `UseMDR` parameter can take the following values:

- `Yes` enables the MDR component.
- `No` disables the MDR component.

If you enable the MDR component, and Kaspersky Security Network is disabled or used in Basic mode, an error message is displayed and the MDR component is not enabled. To enable the MDR component, you must enable KSN in Extended mode.

You can upload or delete the MDR BLOB file using the license key management commands. You can find the BLOB file in the ZIP archive of the MDR configuration file.

```
To upload the BLOB file, execute the following command:
```

```
kesl-control --load-mdr-blob <path to the MDR BLOB>
```

```
To remove the BLOB file, execute the following command:
```

```
kesl-control --remove-mdr-blob
```

Enabling the integration creates a `Mdr_Autostart_Scan` service task that runs once per day.

Managing device network isolation

When integrated with Detection and Response solutions, on the command line, you can:

- Check the network isolation status of a device and view the list of network isolation exclusions.
- Disable network isolation of a device.

To disable network isolation for a device, run the following command:

```
kesl-control [-R] --isolation-off
```

To check the network isolation status and view the list of network isolation exclusions, run the following command:

```
kesl-control [-R] --isolation-stat
```

One of the following network isolation statuses is displayed:

- *Network isolation enabled*.
- *Network isolation disabled*.

Managing Quarantine settings

On the command line, you can configure Quarantine using the `QuarantineSizeLimit`, `QuarantineFillingNotification`, and `QuarantineBackupFolder` settings in the general application settings.

You can change the values of the settings with the help of command line switches or a configuration file that contains all general application settings.

Quarantine settings

Setting	Description	Value
`QuarantineFillingNotification`	The percentage of Quarantine that must be full to generate an event about Quarantine being full. To disable generating events about Quarantine being full, enter 0.	0 to 100 0 – generating events about Quarantine being full is disabled. Default value: 90.

Setting	Description	Value
`QuarantineSizeLimit`	Maximum size of the Quarantine (in megabytes). When the maximum Quarantine size is reached, the application deletes the oldest files. To make the size of Quarantine unlimited, enter 0.	0 to 4000 0 means the Quarantine size is not limited. The default value is 200 if the application is being used in Standard mode or in EDR Agent mode, and 100 if the application is being used in Light Agent mode.
`QuarantineBackupFolder`	Path to the directory in which the Backup and Quarantine objects are stored. You can specify a directory that is different from the default directory. You can use a directory on any device as the directory for storing Backup and Quarantine objects. It is not recommended to assign directories that are located on remote devices, such as those mounted via the Samba and NFS protocols. If the specified directory does not exist or is unavailable, the application uses the default directory.	Default value: /var/opt/kaspersky/kesl/common/objects-backup/ Root privileges are required for access to the default directory.

Managing quarantined files on the command line

When integrated with Detection and Response solutions, on the command line, you can use Quarantine management commands to:

- Put files into Quarantine (only when integrated with Kaspersky Endpoint Detection and Response Optimum or with Kaspersky Managed Detection and Response).
- View information about quarantined files.
- Delete all files or specified files from Quarantine.
- Restore files from Quarantine.

Restoring infected files may lead to a device infection.

Quarantine file

To quarantine a file, run the following command:

```
kesl-control [-Q] --put <path to the file> [--md5] [--sha256] [--save-original-file]
```

where:

- `<path to the file>` is the path to the file that you want to quarantine.
- `--md5` is the MD5 hash of the file that you want to quarantine.
- `--sha256` is the SHA256 hash of the file that you want to quarantine.

- `--save-original-file` keeps the original file. If you do not specify this option, the original file is deleted.

> The original file is deleted only if the user account has permission to delete objects. If the rights are insufficient, a file deletion error message is displayed.

> You can use this command only when integrated with Kaspersky Endpoint Detection and Response Optimum or with Kaspersky Managed Detection and Response.

Viewing information about quarantined files

To view information about quarantined files, run the following command:

```
kesl-control -Q --query ["<filter conditions>"] [-n <number of files>] [--json]
```

where:

- `<filter conditions>` specifies one or more logical expressions in the `< field > < comparison operation > '< value >'` format combined using the `and` logical operator to restrict query results. If you do not specify any filter conditions, the application will display the details of all quarantined files.
- `<number of files>` is the count of the most recent quarantined files that you want to display. If you do not specify the `-n` option, the last 30 files are displayed. Specify 0 to show all files.
- `--json`: output data in JSON format.

The `ObjectId` line displays the numeric ID that the application assigned to the file when quarantining it. This ID is used to perform actions on the file, such as restoring the file or deleting it from Quarantine.

Restore files from Quarantine

To restore a file from Quarantine under its original name to its original location, execute the following command:

```
kesl-control -Q --restore <object identifier>
```

where `<object identifier>` is a numeric ID that the application assigned to the file when it was quarantined.

To restore a file from Quarantine under a new name to a specified directory, execute the following command:

```
kesl-control -Q --restore <object identifier> --file <path to the file>
```

where --file `<path to the file>` is the new name of the file and the path to the directory where you want to save the file.

> You can restore a file from Quarantine to a different directory only if your user has root rights. If your user's rights are insufficient, a file can only be restored to its original location.

> On Astra Linux devices in the closed software environment mode, you can restore a file only under the same account under which it was placed in Backup. When restoring a file, the application creates a directory with MAC label 3 (cnnr flag).

Delete files from Quarantine

To delete selected files from Quarantine, run the following command:

```
kesl-control -Q --mass-remove --query "<filter conditions>"
```

where `<filter conditions>` specifies one or more logical expressions in the <field><comparison operation>'<value>' format combined using the "and" logical operator to restrict query results.

```
Example of deleting files that contain "test" in their names or paths
kesl-control -Q --mass-remove --query "FileName like '%test%'"
```

To delete all files from Quarantine, run the following command:

```
kesl-control -Q --mass-remove
```

Searching for indicators of compromise

> You can scan for indicators of compromise using the IOC Scan task on the command line only when integrated with Kaspersky Endpoint Detection and Response Optimum. When integrated with Kaspersky Endpoint Detection and Response (on-premises) or Kaspersky Endpoint Detection and Response (KATA), the IoC Scan is performed on the side of the relevant Detection and Response solution.

To create, configure, and run an IOC Scan task from the command line, run the following command:

```
kesl-control [-T] --scan-ioc --path <path to the directory or file> [--process on|off] [--hint <regular
expression>] [--arpentry on|off] [--ports on|off] [--system on|off] [--files on|off] [--drives
all|system|critical|custom] [--excludes <list of exclusions>] [--scope <list of directories>] [--action
Skip|QuarantineFile|IsolateHost|ScanCriticalAreas]
```

where:

- `--path <path to the directory or file>` is the path to IOC file or directory with IOC files with the .IOC or .XML extension, which should be used to perform the scan.

  > You can specify multiple paths by separating them with a space. You can also specify both types of paths (path to a file and path to a directory).

- `--process` – enable analysis of processes running on the device.

  Possible arguments:

  - `on` – enable analysis of processes running on the device (default value).
  - `off` – disable analysis of processes running on the device.

  If you do not specify the `--process` option, the application analyzes processes only if the used IOC file specifies the details of these processes (`ProcessItem`).

- `--hint <regular expression>` is the regular expression that matches the full path to the file (`FileItem`) or executable file of the process (`ProcessItem`) to be analyzed.

  You can use the following regular expression elements:

  - meta characters: `. ^ $ |`
  - character classes: digit, alpha, lower, upper, cntrl
  - quantifiers: `* + ? {n} {n,} {n, m}`
  - negation: `[^a-c]`
  - escaped characters: `\a \e \f`, `\n \r \t \v \b`

- `--arpentry` – enable analysis of entries in the ARP table (`ArpEntryItem`).

  Possible arguments:

  - `on` – enable analysis of entries in the ARP table (default value).
  - `off` – disable analysis of entries in the ARP table.

  If you do not specify the `--arpentry` option, the application analyzes the ARP table only if the used IOC file specifies the details of the ARP table (`ArpEntryItem`).

  `--ports` – enable analysis of ports open for connection.

  Possible arguments:

  - `on` – enable analysis of ports open for connection and scan active connections on the device (default value).
  - `off` – disable analysis of ports open for connection and do not scan active connections on the device.

  If you do not specify the `--ports` option, the application only analyzes ports if the used IOC file specifies the details of these ports (`PortItem`).

- `--system` – enable analysis of the system environment.

  Possible arguments:

  - `on` – enable analysis of the system environment (default value).
  - `off` – disable analysis of the system environment.

  If you do not specify the `--system` option, the application analyzes the system environment only if the used IOC file specifies details of the system environment (`SystemInfoItem`).

- `--files` – enable file analysis.

  Possible arguments:

  - `on` – enable file analysis (default value).
  - `off` – disable file analysis.

  If you do not specify the `--files` option, the application analyzes files only if the used IOC file specifies the details of those files (`FileItem`).

- `--drives` – areas to be scanned.

  Possible arguments:

  - `all` – check all available file areas.
  - `system` – scan all files within the root file system.
  - `critical` – scan files in user and system directories (default value).
  - `custom` – scan only files in the areas you specify.

  If you do not specify the `--drives` option, the application analyzes files in user and system directories.

- `--excludes <list of exclusions>` is the list of paths excluded from scanning.

  The exclusions specified by this option are global and are valid regardless of the scope type or directory list. These exclusions take precedence over other command line options, including `--hint` and `--scope`.

  > Exclusions are specified as paths, but cannot contain recursive elements or wildcard characters (e.g. `*`).

  If you do not specify the `--excludes` option, the scan is performed without exclusions.

  You can specify multiple exclusions by separating them with a space.

- `--scope <list of directories>` is the list of additional directories to be scanned.

  > This option is required if you specified the `--drives` argument for the `custom` option.

- `--action` – action performed when indicators of compromise are detected.

Possible arguments:

- `Skip` – the application will not perform any actions with the detected object, but information about it will be saved in the task execution results (default value).
- `QuarantineFile` – the application will quarantine the detected object.
- `IsolateHost` – the application imposes network isolation on the device on which the object is detected.
- `ScanCriticalAreas` – the application will perform a Critical Areas Scan.

  Critical areas scanned by Kaspersky Endpoint Security

  - /lib/systemd
  - /lib/udev
  - /lib/dbus-1.0
  - /usr/local/lib/systemd/user
  - /usr/share/dbus-1
  - /usr/share/gdm/autostart
  - /usr/share/gnome/autostart
  - /var/spool/at
  - /var/spool/at/spool
  - /var/spool/anacron
  - /var/spool/cron
  - /boot
  - /bin
  - /sbin
  - /lib
  - /lib32
  - /lib64
  - /libx32
  - /usr/lib
  - /usr/lib32
  - /usr/lib64
  - /usr/libx32

- ~/.config/autostart
- ~/.config/autostart-scripts
- ~/.config/plasma-workspace/env
- ~/.config/plasma-workspace/shutdown
- ~/.config/lxsession
- ~/.fluxbox/startup
- ~/.kde/Autostart
- /etc

You can specify multiple actions by separating them with commas.

> If you specify the `Skip` argument, do not add any other arguments. The `Skip` argument can only be used on its own.

Managing Execution prevention

Execution prevention allows managing the running of executable files and scripts, as well as opening office format files. Execution prevention manages user access to files with execution prevention rules.

Execution Prevention for objects includes the following tasks:

- *Execution Prevention for objects (EDR Expert (on-premises))* (`KATAEDR_Prevention`)
- *Execution Prevention for objects (EDR Expert (cloud))* (`EDRExpertCloud_Prevention`)
- *Execution prevention for objects (EDR Optimum)* (`EDRO_Prevention`)

By default, *Execution prevention for objects* tasks are not started. If you have added at least one execution prevention rule, the application starts the task.

To view the list of execution prevention rules, run the following command:

```
kesl-control [-T] --get-prevention-state [--kata|cxdr|edro]
```

where:

`--kata`: list of execution prevention rules of the EDR Expert (on-premises) component

`--cxdr`: list of execution prevention rules of the EDR Expert (cloud) component

`--edro`: list of execution prevention rules of the EDR Optimum component

Configuring KUMA integration

On the command line, you can manage the integration of Kaspersky Endpoint Security with Kaspersky Unified Monitoring and Analysis Platform using the predefined task: *Kaspersky Unified Monitoring and Analysis Platform Integration*.

By default, the *Kaspersky Unified Monitoring and Analysis Platform Integration* task is not running. You can start and stop this task manually.

You can configure Kaspersky Unified Monitoring and Analysis Platform Integration settings by editing the settings of the predefined task.

Using the commands for managing the Kaspersky Unified Monitoring and Analysis Platform Integration settings, you can manage certificates that are used for connecting to KUMA servers.

Kaspersky Unified Monitoring and Analysis Platform Integration task

The table describes all available settings and the default values of all the settings that you can specify for the Kaspersky Unified Monitoring and Analysis Platform (`KUMA`) Integration task.

Kaspersky Unified Monitoring and Analysis Platform Integration task settings

Setting	Description	Value
`UseTls`	Enable or disable the server certificate verification for additional protection of the connection to the KUMA server.	`Yes` — use a certificate to further secure the connection to the KUMA server. `No` (default) — do not use a certificate to secure the connection to the KUMA server.
`UseClientCertificate`	Enable and disable two-way authentication to further secure the connection to the KUMA server. If client certificate validation is enabled on the KUMA server side, enable the use of a client certificate and add a client certificate before starting the Kaspersky Unified Monitoring and Analysis Platform Integration task.	`Yes` – use two-way authentication to further secure the connection to the KUMA server. `No` (default value) — do not use two-way authentication.
`ConnectionTimeout`	Maximum time to wait for a connection to the KUMA server in seconds.	Default value: `5`.
The **[Servers.item_#]** section contains the settings of the KUMA server.		
`ServerAddress`	KUMA server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. If you set `UseTls=Yes`, you must specify the fully qualified domain name (FQDN) of the server from the certificate received when purchasing the license to use KUMA.	Default value: `127.0.0.1`.
`ServerPort`	Port to connect to the KUMA server.	Default value: `443`.

Setting	Description	Value
`ServerProtocol`	Protocol for connecting to the KUMA server.	`tcp` (default value) — use the TCP protocol to connect to the KUMA server. `HTTPWithCompression` — use the HTTP protocol with event compression to connect to the KUMA server. `udp` — use the UDP protocol to connect to the KUMA server. When the UDP protocol is selected, the use of certificates to provide connection protection is not supported (the values of the `UseTls`, `UseClientCertificate` and `ConnectionTimeout` settings are ignored), and there are no events about the connection to the KUMA server.
The **[KumaTransferSettings]** section contains settings for sending events to the KUMA server.		
`EventTransferTimeMax`	The maximum delay in sending events to the KUMA server in seconds.	Default value: `30`.

Managing certificates for connecting to the KUMA server

When selecting the UDP protocol, the use of certificates to provide connection protection is not supported.

Managing certificates requires the rights of a user with the Administrator (admin) role.

You can use commands to manage the certificates used for the connection to the KUMA server. You can do the following with certificates:

- Add or replace the server certificate
- Display information about the server certificate
- Remove the server certificate
- Add or replace the client certificate
- Display information about the client certificate
- Remove the client certificate

To add or replace the server certificate, run the following command:

```
kesl-control [-M] --add-kuma-server-certificate <path to the file>
```

where `<path to the file>` is the path to the file that contains the server certificate, in DER or PEM format.

To add or change a client certificate:

1. Run the following command:

   ```
   kesl-control [-M] --add-kuma-client-certificate <path to the file>
   ```

   where `<path to the file>` is the path to the cryptocontainer (PFX archive) containing the client certificate and private key.

2. Enter the crypto-container password

The client certificate is used for additional protection of the connection to the KUMA server if client certificate verification is enabled in the KUMA server settings and in the *Integration with Kaspersky Unified Monitoring and Analysis Platform* task settings the `UseClientCertificate` setting is set to `yes`.

To display certificate information, run the following command:

- for the server certificate:

  ```
  kesl-control [-M] --query-kuma-server-certificate
  ```

- for the client certificate:

  ```
  kesl-control [-M] --query-kuma-client-certificate
  ```

Running the command displays the following certificate information:

- Certificate serial number
- Certificate subject
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA1 and SHA256 certificate fingerprints

To delete the server certificate information, run the following command:

```
kesl-control [-M] --remove-kuma-server-certificate
```

To delete the client certificate information, run the following command:

```
kesl-control [-M] --remove-kuma-client-certificate
```

General settings

In the Administration Console, you can manage general application settings that define the operation of the application as a whole and the operation of individual functions, in the in the policy properties (**General settings**).

General application settings

The table below describes general application settings that govern the operation of the application as a whole and the operation of individual functions.

General application settings

Setting	Description	Values
`SambaConfigPath`	Directory that stores the Samba configuration file. The Samba configuration file is required to ensure that the `AllShared` or `Shared:SMB` values can be used for the `Path` setting. The application must be restarted after this setting is changed.	The standard directory of the SAMBA configuratio on the computer is specified by default. Default value: /etc/samba/smb.conf.
`NfsExportPath`	The directory where the NFS configuration file is stored. The NFS configuration file is required to ensure that the `AllShared` or `Shared:NFS` values can be used for the `Path` setting. The application must be restarted after this setting is changed.	The standard directory of the NFS configuration fil on the computer is specified by default. Default value: /etc/exports.
`TraceFolder`	The directory that stores the application trace files. The application must be restarted after this setting is changed.	Default value: /var/log/kaspersky/kesl. Root privileges are required to access the default t directory. If you specify a different directory, make only the root has read and write permissions to this (`700` or `rwx--------` permissions).
`TraceLevel`	Enable application tracing and the level of detail in the trace files. This setting only enables the generation of application trace files. To generate trace files for the graphical interface and the kesl-control command-line utility, you need to set the LFS_ENABLE_ALL_COMPONENTS_LOGGING environment variable.	`Detailed` – Generate a detailed application trace `MediumDetailed` – Generate an application trace contains informational messages and error messag `NotDetailed` – Generate an application trace file contains error messages. `None` (default value) – Do not generate an applicati file.
`TraceMaxFileCount`	Maximum number of application trace files. The application must be restarted after this setting is changed.	1–10000 Default value: 10.

Setting	Description	Values
`TraceMaxFileSize`	Specifies the maximum size of an application trace file (in megabytes). The application must be restarted after this setting is changed.	1–1000 Default value: 500.
`WdTraceLevel`	Enable Watchdog server tracing and the level of detail in the trace files.	`Detailed` – Generate a detailed Watchdog server `MediumDetailed` – Generate a Watchdog server t that contains informational messages and error me `NotDetailed` – Generate a Watchdog server trac contains error messages. `None` – Do not generate a Watchdog server trace f `Product` (default value) – Set the value equal to th `TraceLevel` value.
`BlockFilesGreaterMaxFileNamePath`	Blocks access to files for which the full path length exceeds the defined settings value specified in bytes. If the length of the full path to the scanned file exceeds the value of this setting, scan tasks skip this file during scanning. This setting only applies to operating systems that do not support fanotify. After changing the value of this setting, the File Threat Protection task needs to be restarted.	4096–33554432 Default value: 16384.
`DetectOtherObjects`	Enable detection of legitimate applications that intruders can use to compromise devices or data.	`Yes`: enable detection of legitimate applications tha can use to compromise devices or data. `No` (default): disable detection of legitimate applica intruders can use to compromise devices or data.
`NamespaceMonitoring`	Enable scanning of namespaces and containers. The application does not scan namespaces and containers unless components for working with containers and namespaces are installed in the operating system.	`Yes` (default value) enables scanning of namespace containers. `No` disables scanning of namespaces and container
`FileBlockDuringScan`	Enabling the file operation intercept mode with blocking access to files for the duration of the scan. The file operation interception mode affects the File Threat Protection and Device Control components, the Execution prevention for objects action and the Removable Drives Scan task.	`Yes` (default value) — Block access to files for the d the scan. `No` to allow access to files during the scan. Request is allowed, scanning is done asynchronously. This mo operation interception has less impact on system p while scanning, but there is a risk that the threat in t might not get disinfected or deleted. This may happ the scan, the process associated with this file mana rename the file before the application can make a d the status of this file. However, the File Threat Prote Device Control, Execution prevention components, Removable Drives Scan task operate in Inform mod regardless of the selected operating mode.
`UseKSN`	Configure Kaspersky Security Network for the application.	`Basic` — Enable use of Kaspersky Security Networ standard mode. `Extended` — Enable use of Kaspersky Security Net extended mode. `No` (default value) — Do not use the Kaspersky Secu Network.

Setting	Description	Values
`CloudMode`	Enable cloud mode. Cloud mode is available if use of KSN is enabled. If you plan to use cloud mode, make sure KSN is available on your device. This setting applies only if the application is used in standard mode.	`Yes` (default value) — Enable the operating mode in Kaspersky Endpoint Security uses a lightweight ver malware databases. `No` (default value) — Use the full version of the malv databases. Cloud mode is disabled automatically if use of KS disabled.
`UseMDR`	Enabling the Managed Detection and Response component for integration with Kaspersky Managed Detection and Response. If you enable the MDR component, and Kaspersky Security Network is disabled or used in Basic mode, an error message is displayed and the MDR component is not enabled. To enable the MDR component, you must enable KSN in Extended mode. This setting is not applicable to devices with an Elbrus CPU.	`Yes` — Enable the Managed Detection and Respons component. `No` (default value) — Disable the Managed Detectio Response component.
`UseEdrOptimum`	Enabling the EDR Optimum component for integration with Kaspersky Endpoint Detection and Response Optimum. This setting is not applicable to devices with an Elbrus CPU.	`Yes` — Enable the EDR Optimum component. `No` (default) — Disable the EDR Optimum componer
`UseProxy`	Enables use of a proxy server by Kaspersky Endpoint Security components. The proxy server can be used for access to Kaspersky activation servers, to update sources for databases and application modules, to Kaspersky Security Network, and when verifying website certificates using the Web Threat Protection component. If Kaspersky Endpoint Security is used in Light Agent mode, the use of a proxy server for connecting to Kaspersky Security Network, the SVM, and the Integration Server is not supported.	`Yes`: enable the use of a proxy server. `No` (default) — Disable the use of a proxy server.

Setting	Description	Values
`ProxyServer`	Address of the proxy server used to connect to the Internet. When connecting via an HTTP proxy, we recommend to use a separate account that is not used to sign in to other systems. An HTTP proxy uses an insecure connection, and the account may be compromised.	Address of the proxy server in one of the following • `[<connection protocol>://]<address o proxy server>:<port>`, if no authentication to connect to the proxy server; • `[<connection protocol>://][<user nam [<password>]@]<address of the proxy s <port>`, if authentication is required when con to the proxy server. When specifying an IPv6 a enter it in square brackets. Connecting to a proxy server over HTTPS is not supported.
`ProxyBypass`	List of addresses for which the proxy server is to be bypassed.	The address is specified in the `<address>[:<port` To specify addresses, you can use masks (`*` symbo comments after a `\` symbol.
`ProxyBypassEdr`	Whether a proxy server is used when connecting to Kaspersky Endpoint Detection and Response Expert (on-premises) integration servers. This setting is not applicable to devices with an Elbrus CPU.	`Yes` not to use a proxy server when connecting to Endpoint Detection and Response Expert (on-prem integration servers. `No` (default value) to use a proxy server when conn Kaspersky Endpoint Detection and Response Exper premise) integration servers.
`ProxyBypassNdr`	Whether a proxy server is used when connecting to Kaspersky Network Detection and Response (KATA) integration servers. This setting is not applicable to devices with an Elbrus CPU.	`Yes` – do not use a proxy server when connecting t Kaspersky Network Detection and Response (KATA servers. `No` (default value) – use a proxy server when conne Kaspersky Network Detection and Response (KATA servers.
`ProxyBypassSandbox`	Whether a proxy server is used when connecting to servers that provide interaction with Sandbox. This setting is not applicable to devices with an Elbrus CPU.	`Yes` to bypass the proxy server when connecting t that provide interaction with Sandbox. `No` (default value) to use the proxy server when co servers that provide interaction with Sandbox.
`MaxEventsNumber`	The maximum number of events stored by the application. When the specified number of events is exceeded, the application deletes the oldest events.	Default value: 500000. If the value is 0, new events are not saved, and old e deleted.
`LimitNumberOfScanFileTasks`	The maximum number of custom scan tasks that a non-privileged user can simultaneously start on the device. This setting does not limit the number of tasks that a user with root privileges or the kesladmin role can start.	0–100000 0 means a non-privileged user cannot start custom Default value: 100.
`UseSyslog`	Enables logging of application events to syslog. Root privileges are required to access syslog.	`Yes`: enable saving events to syslog. `No` (default): disable saving events to syslog.
`EventsStoragePath`	Path to the main file of the event log database. Root privileges are required to access the default event database.	The default value: `/var/opt/kaspersky/kesl/private/storage/`

Setting	Description	Values
`ExcludedMountPoint.item_#`	The mount point to exclude from the scan scope. The exclusion applies to the operation of the File Threat Protection, Anti-Cryptor, and Container Monitoring components and the Removable Drives Scan task, and is also configured in the operation of ODS and ContainerScan scan tasks. You can specify several mount points to be excluded from scans. Mount points must be specified in the same way as they are displayed in the `mount` command output. The `ExcludedMountPoint.item_#` setting is left unspecified by default.	`AllRemoteMounted` — Exclude all remote directori on the device using SMB and NFS protocols from fi interception. `Mounted:NFS` — Exclude all remote directories mou the device using the NFS protocol from file operati interception. `Mounted:SMB` — Exclude all remote directories mou the device using the SMB protocol from file operati interception. `Mounted:<file system type>`: Exclude all moun directories with the specified file system type from operation interception. `/mnt` — Exclude objects in the /mnt mount point (ir subdirectories) from file operation interception. Thi is used as the temporary mount point for removabl `<path that contains the /mnt/user*|/mnt/**/user_share>`: Exclude obj mount points whose names contain the specified m file operation interception.
`MemScanExcludedProgramPath.item_#`	Exclude process memory from scans. The application does not scan the memory of the indicated process.	`<full path to process>` — Exclude objects in t directory from scanning. You can use masks to spec path.
`PowerSaveMode`	Canceling scheduled tasks on a device running on battery power.	`Yes` (default value) skips scheduled tasks when the running on battery power. `No` runs scheduled tasks regardless of whether the running on battery power or not.
`UseOnDemandCPULimit`	Enables CPU usage limits for the *ODS*, *ContainerScan*, and *InventoryScan*-type tasks.	`Yes`: enable the CPU usage limit for *ODS*, *Containe InventoryScan* tasks. `No` (default): disable CPU usage limits for tasks.
`OnDemandCPULimit`	The maximum utilization of all processor cores (as a percentage) when running *ODS*, *ContainerScan*, and *InventoryScan*-type tasks.	Integer value from 10 to 100. Default value: 100.
`BackupSizeLimit`	Maximum Backup size in MB. When the maximum Backup storage size is reached, the application deletes the oldest backup copies of files. To remove the Backup size limit, set 0.	0 to 4000 0–unlimited size. Default value: 0.
`BackupDaysToLive`	Time period for storing objects in the Backup storage (in days). After the specified time has elapsed, the application deletes the oldest backup copies of files. To remove the object retention limit, set 0.	0 to 10000 0–unlimited retention. Default value: 30.
`QuarantineSizeLimit`	Maximum size of the Quarantine (in megabytes). When the maximum Quarantine size is reached, the application deletes the oldest files. To make the size of Quarantine unlimited, enter 0. This setting is not applicable to devices with an Elbrus CPU.	0 to 999999 0 means the Quarantine size is not limited. The default value is 200 if the application is being u Standard mode, and 100 if the application is being u Agent mode.

Setting	Description	Values
`QuarantineFillingNotification`	The percentage of Quarantine that must be full to generate an event about Quarantine being full. To disable generating events about Quarantine being full, enter 0. This setting is not applicable to devices with an Elbrus CPU.	0 to 100 0 – generating events about Quarantine being full is Default value: 90.
`QuarantineBackupFolder`	The path to the directory where backup copies of files and quarantined files are stored. You can change the default directory. If the specified directory does not exist or is unavailable, the application uses the default directory. This setting is not applicable to devices with an Elbrus CPU. The `BackupFolder` setting is used.	The default value: `/var/opt/kaspersky/kesl/common/objects-b` Root privileges are required for access to the de directory.
`BackupFolder`	Path to the Backup directory. You can change the default directory. If the specified directory does not exist or is unavailable, the application uses the default directory.	Default value: `/var/opt/kaspersky/kesl/common/objects-b` Root privileges are required to access the defau Backup storage directory.
`ShowPopUpNotifications`	Enables displaying pop-up notifications in the graphical user interface.	`Yes` (default value) – show pop-up notifications in t graphical user interface. `No` – do not show pop-up notifications in the graph interface.
`InterceptorMode`	The system event interception mechanism used by Kaspersky Endpoint Security: This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.	`UseFanotify` (default) – use the fanotify technolo intercept system events. `UseUpdatableKernelModule` – use an updatable module to intercept system events.
`InterceptorFallbackStrategy`	What the application does if the updatable kernel module fails to start. This setting is applied only on devices running an operating system that supports the fanotify technology.	`FallbackToFanotify` (default) – switch to fanoti system event interception. `FallbackToLimitedMode` – do not use system ev interception. If the application does not use system interception, real-time file scanning is not performe protection level of the device is reduced.

Setting	Description	Values
`InterceptorApplyStrategy`	If the application switches to using the updatable kernel module, the application must be restarted to start the module. This setting lets you specify if you want the application to be restarted automatically or if you prefer to restart the application manually. This setting is applied only on devices running an operating system that supports the fanotify technology.	`RestartServiceAutomatically` automatically re application to start the updatable kernel module. W recommend using this setting. `RestartServiceManually` (default) starts the up kernel module after the application is restarted mar user.
`SystemEventsTransmission`	Enabling the transmission of information about events from third-party applications (which are not Kaspersky solutions). If this setting is enabled, in addition to its own events, Kaspersky Endpoint Security also sends systemd-journald events of third-party applications to the application event log. Access to systemd-journald requires root privileges.	`Yes` enables the transmission of information about journald events of third-party applications to the ap event log. `No` (default) disables the transmission of informatic systemd-journald events of third-party applications application event log.
`UrgentUpdateRestartEnabled`	Automatically restart the application when receiving critical updates after the first 24 hours after installing the application.	`Yes` to automatically restart the application when r critical updates. `No` (default value) not to restart the application wh critical updates.
`CoreDumps`	Enables the creation of a dump file when application failure occurs.	`Yes` to create a dump file when the application cras `No` (default value) not to create a dump file when th application crashes.
`CoreDumpsPath`	Path to the directory where the dump files are stored.	The default value: `/var/opt/kaspersky/kesl/common/dumps` Root privileges are required to access the defau file directory.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Task schedule

The table below describes the task schedule settings that you can manage for all application tasks.

Task start schedule settings

Setting	Description
`RuleType`	Task launch schedule. • `Once`: run the task once. • `Monthly`: run the task on the specified day and time every month. • `Weekly`: run the task on the specified day and time every week. • `Daily`: run the task regularly, at the specified interval in days. • `Hourly`: run the task regularly, at the specified interval in hours, starting on the specified date and time. • `Minutely`: run the task regularly, at the specified interval in minutes, starting at the specified time. • `Manual` – start the task manually. • `PS` – start the task after starting the application. • `BR` – start the task after the application databases have been updated.
`StartTime`	Task start date and time. The format of this setting depends on the `RuleType`. Possible values: • `<year>`: 1970 to 2099 • `<month>`: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC. • `<day of the month>`: 1 to 31 • `<day of the week>`: Mon, Tue, Wed, Thu, Fri, Sat, Sun. • `<hh>`: 0 to 23 • `<mm>`: 0 to 59 • `<ss>`: 0 to 59 • `<interval between runs (in days)>`: 0 to 364 • `<interval between runs (in hours)>`: 0 to 23 • `<interval between runs (in minutes)>`: 0 to 59
`RandomInterval`	Run the task on computers randomly within a certain time interval (from 0 to the specified value). This avoids multiple tasks starting at the same time. Default value: 99 minutes. Possible values: 0 – 999.
`RunMissedStartRules`	Runs a missed task after the application is started. • `Yes` (default value) means that running a missed task is enabled. If the application is stopped or the computer is powered off while a scheduled task is running, Kaspersky Endpoint Security starts that task immediately after the application starts. This helps you make sure critical tasks are never missed. • `No` means that running a missed task is disabled. If the application is stopped or the computer is powered off while a scheduled task is running, the application skips that task. This helps you avoid extra load when starting the application.
`UseWorkingTimeout`	Stops the task upon reaching the maximum task execution time specified by the `WorkingTimeout` setting. The task will be stopped even if it is not completed. The next launch of the task will be performed according to the schedule. • `Yes` – Stop the task when the maximum task execution time has been reached. • `No` (default value) – Do not stop the task when the maximum task execution time has been reached.
`WorkingTimeout`	The maximum task execution time (in minutes) after which the application stops executing the task if `UseWorkingTimeout=Yes`. Default value: 120 minutes. Possible values: 1 – 999.

Configuring proxy server settings

On the command line, you can manage proxy server settings for application components using the `UseProxy`, `ProxyServer`, `ProxyBypass`, `ProxyBypassEdr`, `ProxyBypassNdr` and `ProxyBypassSandbox` general application settings.

You can change the values of the settings with the help of command line switches or a configuration file that contains all general application settings.

The `UseProxy` parameter can take the following values:

- `Yes` enables the use of a proxy server.
- `No` disables the proxy server.

The ProxyServer setting allows specifying proxy server settings in the `<connection protocol>://[<user>[:<password>]@]<proxy server address>:<port number>` format, where:

- `<user>` is a user name for authentication on the proxy server.
- `<password>` is a user password for authentication on the proxy server.
- `<proxy server address>` is the IP address or domain name of the proxy server.
- `<port number>` is the port number of the proxy server.

Connecting to a proxy server over HTTPS is not supported.

When connecting via an HTTP proxy, we recommend to use a separate account that is not used to sign in to other systems. An HTTP proxy uses an insecure connection, and the account may be compromised.

The `ProxyBypass` setting lets you specify a list of addresses that will be connected to without a proxy server. The address is specified in the `<address>[:<port number>]` format. To specify addresses, you can use masks (`*` symbols) and comments (after a \ symbol).

The following settings allow you to configure the use of a proxy server by the EDR Expert (on-premises), NDR (KATA), and Sandbox components, which provide integration with Detection and Response solutions:

- The `ProxyBypassEdr` setting enables or disables the use of a proxy server when connecting to servers that provide integration with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA).
- The `ProxyBypassNdr` setting enables or disables the use of a proxy server when connecting to servers that provide integration with Kaspersky Network Detection and Response (KATA).
- The `ProxyBypassSandbox` setting enables or disables the use of a proxy server when connecting to servers that provide interaction with Sandbox.

These settings can take the following values:

- `Yes` enables the use of a proxy server.
- `No` disables the proxy server.

Configuring Backup settings

On the command line, you can configure Backup settings using the `BackupDaysToLive, BackupSizeLimit` and `QuarantineBackupFolder` settings in the general application settings.

You can change the values of the settings with the help of command line switches or a configuration file that contains all general application settings.

Backup settings

Setting	Description	Value
`BackupDaysToLive`	Time period for storing objects in the Backup storage (in days). After the specified time has elapsed, the application deletes the oldest backup copies of files. To remove the object retention limit, set 0.	0 to 10000 0–unlimited retention. Default value: 30.
`BackupSizeLimit`	Maximum Backup size in MB. When the maximum Backup storage size is reached, the application deletes the oldest backup copies of files. To remove the Backup size limit, set 0.	0 to 4000 0–unlimited size. Default value: 0.
`QuarantineBackupFolder`	The path to the directory where backup copies of files and quarantined files are stored. You can change the default directory. If the specified directory does not exist or is unavailable, the application uses the default directory. This setting is not applicable to devices with an Elbrus CPU. The `BackupFolder` setting is used.	Default value: `/var/opt/kaspersky/kesl/common/objects-backup/` Root privileges are required for access to the default directory.
`BackupFolder`	Path to the Backup directory. You can change the default directory. If the specified directory does not exist or is unavailable, the application uses the default directory.	Default value: `/var/opt/kaspersky/kesl/common/objects-backup/` Root privileges are required to access the default Backup storage directory.

Network traffic scan settings

Network traffic scan settings

Setting	Description	Values
`EncryptedConnectionsScan`	Enables or disables the scanning of encrypted connections. For the FTP protocol, encrypted connections scan is disabled by default.	`Yes` (default value) — Enable encrypted connection scans. `No` — Disable encrypted connection scans. The application does not decrypt the encrypted traffic.
`EncryptedConnectionsScanErrorAction`	Specifies the action to perform when an encrypted connection scan error occurs on a website.	`AddToAutoExclusions` (default value) — Add the domain where an error occurred to the list of domains with scan errors. The application will not monitor encrypted network traffic when this domain is visited. `Disconnect` — Block the network connection.
`CertificateVerificationPolicy`	Specifies the way Kaspersky Endpoint Security checks certificates. If a certificate is self-signed, the application does not perform the additional verification.	`FullCheck` (default value) — The application uses the Internet to check and download the missing chains that are required to verify a certificate. `LocalCheck` — The application does not use the Internet to verify a certificate.
`UntrustedCertificateAction`	The action to take when an unconfirmed certificate is detected.	`Allow` (default value) — Allow network connections established while visiting a domain with an untrusted certificate. `Block` — Block network connections established while visiting a domain with an untrusted certificate.

Setting	Description	Values
`ManageExclusions`	Using exclusions when scanning encrypted traffic.	`Yes` — Do not scan websites specified under `[Exclusions.item_#]` (see below). `No` (default value) — Scan all websites.
`MonitorNetworkPorts`	Specifies the way Kaspersky Endpoint Security monitors network ports.	`Selected` (default value) — Monitor only network ports specified in the `[NetworkPorts.item_#]` section (see below). `All` — Monitor all network ports. Specifying this value may significantly increase an operating system load.
`NetInterceptorMode`	Traffic interception mode by the Kaspersky Endpoint Security application. This setting is not applicable to devices with an Elbrus CPU.	`UseEBPF` — use the eBPF technology to intercept traffic. `UseIPTables` (default value) — use the iptables utility to intercept traffic. To change the traffic interception mode, you need to restart the application. Restarting breaks established network connections.
The **[Exclusions.item_#]** section contains domains excluded from scans. The application does not scan connections established when visiting specified domains.		
`DomainName`	Specifies the domain name.	You can use masks when specifying a domain.
The **[IncomingEndpointsExclusions.item_#]** section contains exclusions for incoming traffic.		
`RemoteIp`	IP address of the remote device, traffic from which is excluded from interception.	
`DestinationPort`	Port on the protected device, traffic to which from remote devices is excluded from interception.	
The **[OutgoingEndpointsExclusions.item_#]** section contains exclusions for outgoing traffic.		
`RemoteIp`	IP address of the remote device, traffic to which is excluded from interception.	
`DestinationPort`	Port on the remote device, traffic to which from the protected device is excluded from interception.	
The **[NetworkPorts.item_#]** section contains the network ports monitored by the application.		
`PortName`	Network port description.	
`Port`	Network port numbers to be monitored by the application.	`1 – 65535`. The default value is not defined.

Configuring global exclusions

You can define mount point exclusions in the command line via the `ExcludedMountPoint.item_#` option in the general application settings.

You can change the value of the setting with the help of command line switches or a configuration file that contains all general application settings.

The `ExcludedMountPoint.item_#` parameter can take the following values:

- `AllRemoteMounted` — Exclude all remote directories mounted on the device using SMB and NFS protocols from file operation interception.
- `Mounted:NFS` — Exclude all remote directories mounted on the device using the NFS protocol from file operation interception.
- `Mounted:SMB` — Exclude all remote directories mounted on the device using the SMB protocol from file operation interception.
- `Mounted:<file system type>`: Exclude all mounted directories with the specified file system type from file operation interception.
- `/mnt` — Exclude objects in the /mnt mount point (including subdirectories) from file operation interception. This directory is used as the temporary mount point for removable drives.
- `<path containing the mask /mnt/user* or /mnt/**/user_share>`: Exclude objects in mount points whose names contain the specified mask from file operation interception.

> Mount points must be specified in the same way as they are displayed in the `mount` command output.

You can specify several mount points to exclude from scanning.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Password protection settings

You can grant or revoke the rights to manage the application by changing settings using command line options or by editing a configuration file.

Password protection settings

Setting	Description	Value
`StopProtection`	Disabling protection components.	`Yes` allows the user to perform the action. `No` forbids the user from performing an action.
`StopSecurityControl`	Disabling control components	
`StartProtection`	Enabling protection components	
`StartSecurityControl`	Enabling control components	
`ApplicationSettings`	Configuring the application	
`ViewReports`	Viewing reports	
`RestoreFromBackup`	Restoring from Backup	
`RemoveLicenseKey`	Remove key	
`AddLicense`	Adding a key	
`DisablePolicy`	Disabling the Kaspersky Security Center policy	

Application settings in the Administration Console

You use a policy to configure Kaspersky Endpoint Security. Detailed information about application components is provided in the corresponding sections.

Database update

In the Administration Console, you can update databases using the Update task.

You can create and run update user tasks. You can manage update settings by editing the settings of the tasks.

In the properties of the Update task, in the **Update sources** and **Settings** sections, you can manage the settings listed in the table below.

Update sources for the Update task section

Setting	Description

Update source	This table contains a list of database update sources. During the update process, the application accesses update sources in the order they appear in the table.
	The table contains the following columns:
	• **Source address** is the address of the update source:
	  • **Kaspersky update servers**, where database updates for Kaspersky applications are published (default value).
	  • **Kaspersky Security Center** – Kaspersky Security Center Administration Server.
	  • Other sources from the local or global network added by the user: HTTP, HTTPS, or FTP servers or directories on local network servers.
	• **Status** indicates whether the update source is used in the task (**In use** or **Not in use**). You can change the status by selecting or clearing the **Use this source** check box in the **Update source** window that opens when you click the **Edit** button.
	You can add, edit, delete, move up, or move down update sources in the table.

Update task settings section

Setting	Description
Timeout for response from the update source (sec)	The maximum period of time that the application waits for a response from the selected update source (in seconds). When no response has arrived by this time, an event involving a loss of communication with the update source is logged in the task log. Possible values: 0–120. If 0 is specified, the period of time that the application waits for a response from the selected source is unlimited. Default value: 10 seconds.
Application update download mode	In the drop-down list, you can select how you want the automatically installed updates (autopatches) to be downloaded: • **Do not download**. When this item is selected, autopatches are not automatically downloaded. • **Download only**. When this list item is selected, autopatches are automatically downloaded, but not installed on client devices (default setting). • **Download and install**. When this list item is selected, autopatches are automatically downloaded and installed on client devices. After an autopatch is installed, the application restarts automatically.

Host Threat Protection

File Threat Protection

In the Administration Console, you can manage File Threat Protection in the policy properties (**Essential Threat Protection → File Threat Protection**).

File Threat Protection component settings

Setting	Description
Enable File Threat Protection	This check box enables or disables File Threat Protection component on all managed devices. This check box is selected by default.
File Threat Protection mode	In this drop-down list, you can select the File Threat Protection component mode: • **Smart check** (default value) – scan a file when there is an attempt to open it and scan it again when there is an attempt to close it if the file has been modified. If a process accesses and modifies a file multiple times in a certain period, the application scans the file again only when the process closes it for the last time. • **When opened** – scan the file on an attempt to open it for reading, execution, or modification. • **When opened and modified** – scan a file on an attempt to open it, and scan it again on an attempt to close it if the file has been modified.
Scan	This group of settings contains buttons that open windows where you can configure the scan scopes and scan settings.
Actions on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Actions on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

Scan scopes window

The table contains the scan scopes. The application will scan files and directories located in the paths specified in the table. By default, the table contains one scan scope that includes all directories of the local file system.

Scan scope settings

Setting	Description
Scope name	Scan scope name.
Path	Path to the directory that the application scans.
Status	The status indicates whether the application scans this scope.

You can **add**, **edit**, **delete**, **move up**, and **move down** items in the table.

Clicking the **Move down** button moves the selected item down in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Delete** button excludes the selected scope from scans.

This button is available if at least one scan scope is selected in the table.

The selected element's settings are changed in a separate window.

Clicking the **Add** button opens a window where you can specify the new item settings.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

New scan scope window

In this window, you can add and configure scan scopes.

Scan scope settings

Setting	Description
Scan scope name	Field for entering the scan scope name. This name will be displayed in the table in the Scan scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables scans of this scope by the application. If this check box is selected, the application processes this scan scope. If this check box is cleared, the application does not process this scan scope. You can later include this scope in the component settings by selecting the check box. This check box is selected by default.

Setting	Description
File system, access protocol, and path	The settings block lets you set the scan scope. You can select the file system type in the drop-down list of file systems: • **Local** (default value) – local directories. If this item is selected, you need to indicate the path to the local directory. • **Mounted** – Mounted remote or local directories. If this item is selected, you need to indicate the protocol or name of the file system. • **Shared** — The protected server's file system resources accessible via the Samba or NFS protocol. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols. • **All shared** — All of the protected server's file system resources accessible via the Samba and NFS protocols.
	If **Shared** or **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want to add to the scan scope. You can use masks and tags to specify the path. The **/** path is specified by default – the application scans all directories of the local file system. If the **Local** type is selected in the drop-down list of file systems, and the path is not specified, the application scans all directories of the local file system.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the scan scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks for the objects that the application scans. By default the list contains the ***** mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Scan settings window

In this window, you can configure file scan settings while File Threat Protection is enabled.

File Threat Protection settings

Setting	Description
Scan archives	This check box enables or disables scan of archives. If this check box is selected, Kaspersky Endpoint Security scans archives. To scan an archive, the application has to unpack it first, which may slow down scanning. You can reduce the duration of archive scans by enabling and configuring the **Skip file that is scanned for longer than (sec)** and **Skip file larger than (MB)** settings in the **General scan settings** section. If this check box is cleared, Kaspersky Endpoint Security does not scan archives. This check box is cleared by default.
Scan SFX archives	This check box enables or disables *self-extracting archive* scans. Self-extracting archives are archives that contain an executable extraction module. If this check box is selected, Kaspersky Endpoint Security scans self-extracting archives. If this check box is cleared, Kaspersky Endpoint Security does not scan self-extracting archives. This check box is available if the **Scan archives** check box is unchecked. This check box is cleared by default.
Scan mail databases	This check box enables or disables scans of mail databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail applications. If this check box is selected, Kaspersky Endpoint Security scans mail database files. If this check box is cleared, Kaspersky Endpoint Security does not scan mail database files. This check box is cleared by default.

Setting	Description
Scan mail format files	This check box enables or disables scan of files of plain-text email messages. If this check box is selected, Kaspersky Endpoint Security scans plain-text messages. If this check box is cleared, Kaspersky Endpoint Security does not scan plain-text messages. This check box is cleared by default.
Skip text files	Temporary exclusion of files in text format from scans. If the check box is selected, Kaspersky Endpoint Security does not scan text files if they are used by the same process within 10 minutes after the most recent scan. This setting makes it possible to optimize scans of application logs. If this check box is unselected, Kaspersky Endpoint Security scans text files. This check box is cleared by default. This setting is applied if you use system event interception mechanism based on fanotify. When using an updatable kernel module, the scan is optimized by using the scan result cache.
Skip database journal files	Temporarily excluding database journal files from scanning. If this check box is selected, the application does not scan database journal files if the journal file is reused by the same process within 10 minutes after the most recent scan. This setting makes it possible to optimize scans of database journal files. If this check box is cleared, the application scans database journal files. This check box is cleared by default. This setting is applied if you use system event interception mechanism based on fanotify. When using an updatable kernel module, the scan is optimized by using the scan result cache.
Skip file that is scanned for longer than (sec)	In this field, you can specify the maximum time to scan a file, in seconds. After the specified time, Kaspersky Endpoint Security stops scanning the file. Possible values: 0–9999. If the value is set to 0, the scan time is unlimited. Default value: 60.
Skip file larger than (MB)	In this field, you can specify the maximum size of a file to scan, in megabytes. Possible values: 0–999999. If the value is set to 0, Kaspersky Endpoint Security scans files of any size. Default value: 0.
Log clean objects	This check box enables or disables the logging of *ObjectProcessed* type events. If this check box is selected, Kaspersky Endpoint Security logs *ObjectProcessed* type events for all scanned objects. If this check box is cleared, Kaspersky Endpoint Security does not log *ObjectProcessed* type events. This check box is cleared by default.
Log unprocessed objects	This check box enables or disables the logging *ObjectNotProcessed* type events if a file cannot be processed during a scan. If this check box is selected, Kaspersky Endpoint Security logs *ObjectNotProcessed* type events. If this check box is cleared, Kaspersky Endpoint Security does not log *ObjectNotProcessed* type events. This check box is cleared by default.
Log packed objects	This check box enables or disables the logging of *PackedObjectDetected* type events for all packed objects that are detected. If this check box is selected, Kaspersky Endpoint Security logs *PackedObjectDetected* type events. If this check box is cleared, Kaspersky Endpoint Security does not log *PackedObjectDetected* type events. This check box is cleared by default.
Use iChecker technology	This check box enables or disables scan of only new and modified since the last scan files. If the check box is selected, Kaspersky Endpoint Security scans only new or modified since the last scan files. If the check box is cleared, Kaspersky Endpoint Security scans files regardless to the date of creation or modification. This check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. This check box is selected by default.

Setting	Description
Heuristic analysis level	If the **Use heuristic analysis** check box is selected, you can select the heuristic analysis level in the drop-down list: • **Light** is the least detailed scan with minimal system load. • **Medium** is a medium scan with balanced system load. • **Deep** is the most detailed scan with maximum system load. • **Recommended** (default value) is the optimal level recommended by Kaspersky experts. It ensures an optimal combination of protection quality and impact on the performance of the protected devices.

Actions on threat detection window

In this window, you can configure actions to be performed by Kaspersky Endpoint Security on detected infected objects:

File Threat Protection settings

Setting	Description
Actions on threat detection	You can select the actions that the application performs on a detected infected object: • **Disinfect; delete if disinfection is not possible** (default). If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. • **Disinfect; block if disinfection fails**. If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application blocks access to the infected object. • **Block**. If you select this action, the application blocks access to the infected object. When an infected object is disinfected or deleted, a copy of the infected object is placed in Backup.

File Threat Protection exclusions

A *protection exclusion* is a set of conditions under which Kaspersky Endpoint Security will not scan objects for viruses and other malware. You can also exclude objects by masks and threat names, and configure exclusions for processes.

In the Administration Console, you can configure File Threat Protection exclusions in the policy properties (**Essential Threat Protection → File Threat Protection exclusions**).

Settings of scan exclusions

Group of settings	Description
Exclusions	This group of settings contains the **Configure** button. Clicking this button opens the Exclusion scopes window. In this window, you can define the list of scopes to be excluded from scan.
Exclusions by mask	This group of settings contains the **Configure** button, which opens the Exclusions by mask window. In this window, you can configure the exclusion of objects from scans by name mask.
Exclusions by threat name	This group of settings contains the **Configure** button, which opens the Exclusions by threat name window. In this window, you can configure the exclusion of objects from scans based on threat name.
Exclusions by process	This group of settings contains the **Configure** button, which opens the Exclusions by process window. In this window, you can exclude the activity of processes.

Exclusion scopes window

This window contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table.

Exclusion scope settings

Setting	Description
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from scan.
Status	The status indicates whether the application uses this exclusion.

By default, the table of exclusion scopes is empty. You can add, edit, and delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

New exclusion scope window

In this window, you can add and configure scan exclusion scopes.

Exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the Exclusion scopes window. The entry field must not be blank.
Use this scope	The check box enables or disables exclusion of the scope from scan when the application is running. If this check box is selected, the application excludes this area during scans. If this check box is cleared, the application includes this area in the scan scope. You can later exclude this scope by selecting the check box. This check box is selected by default.
File system, access protocol, and path	The settings block lets you set the exclusion scope. In the drop-down list of file systems, you can select the type of file system of the directories to be excluded from scans: • **Local**, for local directories. • **Mounted** – mounted directories. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
	If **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want add to the exclusion scope. You can use masks and tags to specify the path. The **/** path is specified by default. The application excludes all directories of the local file system from scan.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the exclusion scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks of the objects that the application excludes from scan. Masks are only applied to objects in the directory specified in the path field. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Exclusions by mask window

You can configure scan exclusions for objects by name mask. The application will not scan files whose names contain the specified mask. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans.

Examples:
The `*.txt` mask refers to all text files.
The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

You can enable the merging of the list of exclusions when inherited by child policies. If you want to merge list items, select the **Merge inherited values** check box. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.

Exclusions by threat name window

You can configure the exclusion of objects from scans based on threat name. The application will not block the specified threats. By default, the list of threat names is empty.

You can add, edit, and delete threat names.

You can enable the merging of the list of exclusions when inherited by child policies. If you want to merge list items, select the **Merge inherited values** check box. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.

Exclusions by process window

This window contains per-process exclusion scopes. The exclusion scope for exclusion by process lets you exclude from scans the activity of the indicated process and files modified by the indicated process. By default, the list includes two exclusion scopes that contain paths to the Network Agents. You can remove these exclusions, if necessary.

Exclusion scope settings for exclusion by process

Setting	Description
Merge inherited values	This check box enables or disables the merging of the list when inherited in child policies. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.
Exclusion scope name	Exclusion scope name.
Path	Full path to excluded process.
Status	The status indicates whether the application uses this exclusion.

You can add, edit, or delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

Trusted process window

In this window, you can add and configure exclusion scopes for exclusion by process.

Exclusion scope settings for exclusion by process

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in a table in the Exclusions by process window. The entry field must not be blank.
Path to excluded process	Full path to the process you want to exclude from scans. If the updatable kernel module is used for system event interception, the specified process is excluded from interception in all namespaces.
Apply to child processes	Exclude child processes of the excluded process indicated by the **Path to excluded process** setting. This check box is cleared by default.
Use this scope	The check box enables or disables this exclusion scope. If this check box is selected, the application excludes this area during scans. If this check box is cleared, the application includes this area in the scan scope. You can later exclude this scope by selecting the check box. This check box is selected by default.
Path to modified files	This group of settings lets you set scan exclusions for files modified by the process. In the drop-down list of file systems, you can select the type of file system of the directories to be excluded from scans: • **Local**, for local directories. If this item is selected, you need to indicate the path to the local directory. • **Mounted** – Mounted remote or local directories. If this item is selected, you need to indicate the protocol or name of the file system. • **Shared** — The protected server's file system resources accessible via the Samba or NFS protocol. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols. • **All shared** — All of the protected server's file system resources accessible via the Samba and NFS protocols. If **Mounted** or **Shared** is selected in the drop-down list of file systems, then you can select the remote access protocol in the drop-down list of access protocols: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below. If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want add to the exclusion scope. You can use masks to specify the path. The entry field must not be blank.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the exclusion scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks of the objects that the application excludes from scan. Masks are only applied to objects in the directory specified in the **Path to modified files** field. You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Malware Scan

In the Administration Console, you can scan for malware using the *Malware Scan* task.

You can run an automatically created group task and also create and run user tasks for scanning. You can manage scan settings by editing the settings of the tasks.

In the properties of the *Search for malware* task, in the **Settings** section you can manage the settings listed in the table below.

Malware Scan task settings

Setting	Description
Scan	This group of settings contains buttons that open windows where you can configure the scan scopes, scan scope settings, and scan settings.
Actions on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Actions on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

In the properties of the *Search for malware* task, in the **Exclusions** section, you can customize exclusion scopes, exclusions by mask and by threat name.

Scan scopes window

The table contains the scan scopes. The application will scan files and directories located in the paths specified in the table. By default, the table contains one scan scope that includes all directories of the local file system.

Scan scope settings

Setting	Description
Scope name	Scan scope name.
Path	Path to the directory that the application scans.
Status	The status indicates whether the application scans this scope.

You can **add**, **edit**, **delete**, **move up**, and **move down** items in the table.

Clicking the **Move down** button moves the selected item down in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Delete** button excludes the selected scope from scans.

This button is available if at least one scan scope is selected in the table.

The selected element's settings are changed in a separate window.

Clicking the **Add** button opens a window where you can specify the new item settings.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

<New scan scope> window

In this window, you can add and configure scan scopes.

Scan scope settings

Setting	Description
Scan scope name	Field for entering the scan scope name. This name will be displayed in the table in the Scan scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables scans of this scope by the application. If this check box is selected, the application processes this scan scope. If this check box is cleared, the application does not process this scan scope. You can later include this scope in the component settings by selecting the check box. This check box is selected by default.
File system, access protocol, and path	The settings block lets you set the scan scope. You can select the file system type in the drop-down list of file systems: • **Local** (default value) – local directories. If this item is selected, you need to indicate the path to the local directory. • **Mounted** – Mounted remote or local directories. If this item is selected, you need to indicate the protocol or name of the file system. • **Shared** — The protected server's file system resources accessible via the Samba or NFS protocol. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols. • **All shared** — All of the protected server's file system resources accessible via the Samba and NFS protocols.
	If **Shared** or **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want to add to the scan scope. You can use masks and tags to specify the path. The **/** path is specified by default – the application scans all directories of the local file system. If the **Local** type is selected in the drop-down list of file systems, and the path is not specified, the application scans all directories of the local file system.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the scan scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks for the objects that the application scans. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Scan scope settings window

In this window, you can configure the scan settings for the Malware Scan task. The application allows you to scan files, boot sectors, device memory, and startup objects.

Scan scope settings

Setting	Description
Scan files	This check box enables or disables file scans. If the check box is selected, the application scans the files. If the check box is cleared, the application does not scan the files. This check box is selected by default.
Scan boot sectors	This check box enables or disables boot sector scans. If the check box is selected, the application scans the boot sectors. If the check box is cleared, the application does not scan the boot sectors. This check box is cleared by default.
Scan kernel memory and running processes	This check box enables or disables device memory scan. If the check box is selected, the application scans kernel memory and running processes. If the check box is cleared, the application does not scan kernel memory and running processes. This check box is cleared by default.
Scan startup objects	This check box enables or disables startup object scans. If the check box is selected, the application scans startup objects. If the check box is cleared, the application does not scan startup objects. This check box is cleared by default.
Devices to scan	This group of settings contains the **Configure** button. Clicking this button opens the **Scan scopes** window, where you can specify the devices whose boot sectors must be scanned.
Use global exclusions	The check box enables or disables the exclusion of the mount points specified in global exceptions while the application is running. If this check box is selected, the application excludes configured mount points from scans. This check box is selected by default.
Use File Threat Protection exclusions	This check box enables or disables the use of configured File Threat Protection exclusions when the application is running. If the check box is selected, the application does not scan the objects specified in the exclusions for the File Threat Protection component. This check box is selected by default.

Scan scopes window

The table contains name masks of the devices, whose boot sectors the application must scan. By default, the table contains the **/**** device name mask (all devices).

You can add, edit, and delete items in the table.

Scan settings window

In this window, you can configure the file scan settings for the task.

Scan settings

Setting	Description
Scan archives	This check box enables or disables scan of archives. If the check box is selected, the application scans the archives. To scan an archive, the application has to unpack it first, which may slow down scanning. You can reduce the duration of archive scans by configuring the **Skip file that is scanned for longer than (sec)** and **Skip file larger than (MB)** settings in the **General scan settings** section. If the check box is cleared, the application does not scan the archives. This check box is selected by default.

Setting	Description
Scan SFX archives	This check box enables or disables *self-extracting archive* scans. Self-extracting archives are the archives that contain an executable extraction module. If the check box is selected, the application scans self-extracting archives. If the check box is cleared, the application does not scan self-extracting archives. This check box is available if the **Scan archives** check box is cleared. This check box is selected by default.
Scan mail databases	This check box enables or disables scans of mail databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail applications. If the check box is selected, the application scans mail database files. If the check box is cleared, the application does not scan mail database files. This check box is cleared by default.
Scan mail format files	This check box enables or disables scan of files of plain-text email messages. If this check box is selected, the application scans plain-text messages. If this check box is cleared, the application does not scan plain-text messages. This check box is cleared by default.
Skip file that is scanned for longer than (sec)	In this field, you can specify the maximum time to scan a file, in seconds. After the specified time, the application stops scanning the file. Possible values: 0–9999. If the value is set to 0, the scan time is unlimited. Default value: 0.
Skip file larger than (MB)	In this field, you can specify the maximum size of a file to scan, in megabytes. Possible values: 0–999999. If the value is set to 0, the application scans files of any size. Default value: 0.
Log clean objects	This check box enables or disables the logging of *ObjectProcessed* type events. If this check box is selected, the application logs events of the *ObjectProcessed* type for all scanned objects. If this check box is cleared, the application does not log events of the *ObjectProcessed* type for any scanned object. This check box is cleared by default.
Log unprocessed objects	This check box enables or disables the logging *ObjectNotProcessed* type events if a file cannot be processed during a scan. If this check box is selected, the application logs the events of the *ObjectNotProcessed* type. If this check box is cleared, the application does not log the events of the *ObjectNotProcessed* type. This check box is cleared by default.
Log packed objects	This check box enables or disables the logging of *PackedObjectDetected* type events for all packed objects that are detected. If this check box is selected, the application logs the events of the *PackedObjectDetected* type. If this check box is cleared, the application does not log the events of the *PackedObjectDetected* type. This check box is cleared by default.
Use iChecker technology	This check box enables or disables scan of only new and modified since the last scan files. If the check box is selected, the application scans only new files or the files modified since the last scan. If the check box is cleared, the application scans the files regardless of the creation or modification date. This check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. This check box is selected by default.

Setting	Description
Heuristic analysis level	If the **Use heuristic analysis** check box is selected, you can select the heuristic analysis level in the drop-down list: • **Light** is the least detailed scan with minimal system load. • **Medium** is a medium scan with balanced system load. • **Deep** is the most detailed scan with maximum system load. • **Recommended** (default) is the optimal level recommended by Kaspersky experts. It ensures an optimal combination of protection quality and impact on the performance of the protected devices.
Do not run multiple scan tasks at the same time	Postponed start of scan tasks if a scan is already running. Kaspersky Endpoint Security will enqueue new scan tasks if the current scan continues. This helps optimize the load on the computer. For example, let's assume that the application has started a Full Scan task according to the schedule. If a user attempts to start a quick scan from the application interface, Kaspersky Endpoint Security will enqueue this quick scan task and then automatically start this task after the Full Scan task is finished. This check box is cleared by default.

Actions on threat detection window

In this window, you can configure actions to be performed by Kaspersky Endpoint Security on detected infected objects:

Actions on threat detection

Setting	Description
Actions on threat detection	You can select the action that the application performs on a detected infected object: • **Disinfect; delete if disinfection is not possible** (default). If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. • **Disinfect; inform if disinfection fails**. If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. • **Inform**. If you select this action, the application creates a record about the infected object in the log.

Exclusions section

Scan exclusion is a set of conditions. When these conditions are met, Kaspersky Endpoint Security does not scan the objects for viruses and other malware. You can also exclude objects from scans by masks and threat names.

Settings of scan exclusions

Group of settings	Description
Exclusion scopes	This group of settings contains the **Configure** button. Clicking this button opens the **Exclusion scopes** window. In this window, you can define the list of scopes to be excluded from scans.
Exclusions by mask	This group of settings contains the **Configure** button, which opens the Exclusions by mask window. In this window, you can configure the exclusion of objects from scans by name mask.
Exclusions by threat name	This group of settings contains the **Configure** button, which opens the Exclusions by threat name window. In this window, you can configure the exclusion of objects from scans based on threat name.

Exclusion scopes window

This window contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table.

Exclusion scope settings

Setting	Description
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from scan.
Status	The status indicates whether the application uses this exclusion.

By default, the table of exclusion scopes is empty. You can add, edit, and delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

New exclusion scope window

In this window, you can add and configure scan exclusion scopes.

Exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the Exclusion scopes window. The entry field must not be blank.
Use this scope	The check box enables or disables exclusion of the scope from scan when the application is running. If this check box is selected, the application excludes this area during scans. If this check box is cleared, the application includes this area in the scan scope. You can later exclude this scope by selecting the check box. This check box is selected by default.
File system, access protocol, and path	The settings block lets you set the exclusion scope. In the drop-down list of file systems, you can select the type of file system of the directories to be excluded from scans: • **Local**, for local directories. • **Mounted** – mounted directories. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
	If **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want add to the exclusion scope. You can use masks and tags to specify the path. The **/** path is specified by default. The application excludes all directories of the local file system from scan.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the exclusion scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks of the objects that the application excludes from scan. Masks are only applied to objects in the directory specified in the path field. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the * (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Exclusions by mask window

You can configure scan exclusions for objects by name mask. The application will not scan files whose names contain the specified mask. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans.

Examples:
The `*.txt` mask refers to all text files.
The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

Exclusions by threat name window

You can configure the exclusion of objects from scans based on threat name. The application will not block the specified threats. By default, the list of threat names is empty.

You can add, edit, and delete threat names.

Critical Areas Scan

In the Administration Console, you can perform a critical areas scan of the operating system of a protected device using the *Critical Areas Scan* task.

You can create and run custom critical areas scan tasks. You can manage scan settings by editing the settings of the tasks.

In the properties of the *Critical Areas Scan* task, in the **Settings** section, you can manage the settings listed in the table below.

Critical Areas Scan task settings

Setting	Description
Scan	This group of settings contains buttons that open windows where you can configure the scan scopes, scan scope settings, and scan settings.
Actions on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Actions on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

In the properties of the *Critical Areas Scan* task, in the **Exclusions** section, you can customize exclusion scopes, exclusions by mask and by threat name.

Scan scopes window

The table contains the scan scopes. The application will scan files and directories located in the paths specified in the table. By default, the table contains one scan scope that includes all directories of the local file system.

Scan scope settings

Setting	Description
Scope name	Scan scope name.
Path	Path to the directory that the application scans.
Status	The status indicates whether the application scans this scope.

You can **add**, **edit**, **delete**, **move up**, and **move down** items in the table.

Clicking the **Move down** button moves the selected item down in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Delete** button excludes the selected scope from scans.

This button is available if at least one scan scope is selected in the table.

The selected element's settings are changed in a separate window.

Clicking the **Add** button opens a window where you can specify the new item settings.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

New scan scope window

In this window, you can add and configure scan scopes.

Scan scope settings

Setting	Description
Scan scope name	Field for entering the scan scope name. This name will be displayed in the table in the Scan scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables scans of this scope by the application. If this check box is selected, the application processes this scan scope. If this check box is cleared, the application does not process this scan scope. You can later include this scope in the component settings by selecting the check box. This check box is selected by default.

Setting	Description
File system, access protocol, and path	The settings block lets you set the scan scope. You can select the file system type in the drop-down list of file systems: • **Local** (default value) – local directories. If this item is selected, you need to indicate the path to the local directory. • **Mounted** – Mounted remote or local directories. If this item is selected, you need to indicate the protocol or name of the file system. • **Shared** — The protected server's file system resources accessible via the Samba or NFS protocol. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols. • **All shared** — All of the protected server's file system resources accessible via the Samba and NFS protocols.
	If **Shared** or **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want to add to the scan scope. You can use masks and tags to specify the path. The **/** path is specified by default – the application scans all directories of the local file system. If the **Local** type is selected in the drop-down list of file systems, and the path is not specified, the application scans all directories of the local file system.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the scan scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks for the objects that the application scans. By default the list contains the ***** mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Scan scope settings window

In this window, you can configure the scan settings for the Critical Areas Scan task. The application allows you to scan files, boot sectors, startup objects, process memory, and kernel memory.

Scan scope settings

Setting	Description
Scan files	This check box enables or disables file scans. If this check box is selected, Kaspersky Endpoint Security will scan files. If this check box is unchecked, Kaspersky Endpoint Security will not scan files. This check box is cleared by default.
Scan boot sectors	This check box enables or disables boot sector scans. If this check box is selected, Kaspersky Endpoint Security will scan boot sectors. If this check box is unchecked, Kaspersky Endpoint Security will not scan boot sectors. This check box is selected by default.
Scan kernel memory and running processes	This check box enables or disables device memory scan. If the check box is selected, Kaspersky Endpoint Security scans kernel memory and running processes. If the check box is cleared, Kaspersky Endpoint Security does not scan kernel memory and running processes. This check box is selected by default.
Scan startup objects	This check box enables or disables startup object scans. If this check box is selected, Kaspersky Endpoint Security will scan startup objects. If this check box is unchecked, Kaspersky Endpoint Security will not scan startup objects. This check box is selected by default.
Devices to scan	This group of settings contains the **Configure** button. Clicking this button opens the Scan scopes window, where you can specify the devices whose boot sectors must be scanned.

Setting	Description
Use global exclusions	The check box enables or disables the exclusion of the mount points specified in global exceptions while the application is running. If this check box is selected, the application excludes configured mount points from scans. This check box is selected by default.
Use File Threat Protection exclusions	This check box enables or disables the use of configured File Threat Protection exclusions when the application is running. If the check box is selected, the application does not scan the objects specified in the exclusions for the File Threat Protection component. This check box is selected by default.

Scan scopes window

The table contains name masks of the devices, whose boot sectors the application must scan. By default, the table contains the **/**** device name mask (all devices).

You can add, edit, and delete items in the table.

Scan settings window

In this window, you can configure the file scan settings for the task.

Scan settings

Setting	Description
Scan archives	This check box enables or disables scan of archives. If the check box is selected, the application scans the archives. To scan an archive, the application has to unpack it first, which may slow down scanning. You can reduce the duration of archive scans by configuring the **Skip file that is scanned for longer than (sec)** and **Skip file larger than (MB)** settings in the **General scan settings** section. If the check box is cleared, the application does not scan the archives. This check box is selected by default.
Scan SFX archives	This check box enables or disables *self-extracting archive* scans. Self-extracting archives are the archives that contain an executable extraction module. If the check box is selected, the application scans self-extracting archives. If the check box is cleared, the application does not scan self-extracting archives. This check box is available if the **Scan archives** check box is cleared. This check box is selected by default.
Scan mail databases	This check box enables or disables scans of mail databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail applications. If the check box is selected, the application scans mail database files. If the check box is cleared, the application does not scan mail database files. This check box is cleared by default.
Scan mail format files	This check box enables or disables scan of files of plain-text email messages. If this check box is selected, the application scans plain-text messages. If this check box is cleared, the application does not scan plain-text messages. This check box is cleared by default.
Skip file that is scanned for longer than (sec)	In this field, you can specify the maximum time to scan a file, in seconds. After the specified time, the application stops scanning the file. Possible values: 0–9999. If the value is set to 0, the scan time is unlimited. Default value: 0.
Skip file larger than (MB)	In this field, you can specify the maximum size of a file to scan, in megabytes. Possible values: 0–999999. If the value is set to 0, the application scans files of any size. Default value: 0.

Setting	Description
Log clean objects	This check box enables or disables the logging of *ObjectProcessed* type events. If this check box is selected, the application logs events of the *ObjectProcessed* type for all scanned objects. If this check box is cleared, the application does not log events of the *ObjectProcessed* type for any scanned object. This check box is cleared by default.
Log unprocessed objects	This check box enables or disables the logging *ObjectNotProcessed* type events if a file cannot be processed during a scan. If this check box is selected, the application logs the events of the *ObjectNotProcessed* type. If this check box is cleared, the application does not log the events of the *ObjectNotProcessed* type. This check box is cleared by default.
Log packed objects	This check box enables or disables the logging of *PackedObjectDetected* type events for all packed objects that are detected. If this check box is selected, the application logs the events of the *PackedObjectDetected* type. If this check box is cleared, the application does not log the events of the *PackedObjectDetected* type. This check box is cleared by default.
Use iChecker technology	This check box enables or disables scan of only new and modified since the last scan files. If the check box is selected, the application scans only new files or the files modified since the last scan. If the check box is cleared, the application scans the files regardless of the creation or modification date. This check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. This check box is selected by default.
Heuristic analysis level	If the **Use heuristic analysis** check box is selected, you can select the heuristic analysis level in the drop-down list: • **Light** is the least detailed scan with minimal system load. • **Medium** is a medium scan with balanced system load. • **Deep** is the most detailed scan with maximum system load. • **Recommended** (default) is the optimal level recommended by Kaspersky experts. It ensures an optimal combination of protection quality and impact on the performance of the protected devices.
Do not run multiple scan tasks at the same time	Postponed start of scan tasks if a scan is already running. Kaspersky Endpoint Security will enqueue new scan tasks if the current scan continues. This helps optimize the load on the computer. For example, let's assume that the application has started a Full Scan task according to the schedule. If a user attempts to start a quick scan from the application interface, Kaspersky Endpoint Security will enqueue this quick scan task and then automatically start this task after the Full Scan task is finished. This check box is cleared by default.

Actions on threat detection window

In this window, you can configure actions to be performed by Kaspersky Endpoint Security on detected infected objects:

Actions on threat detection

Setting	Description
Actions on threat detection	You can select the action that the application performs on a detected infected object: • **Disinfect; delete if disinfection is not possible** (default). If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. • **Disinfect; inform if disinfection fails**. If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. • **Inform**. If you select this action, the application creates a record about the infected object in the log.

Exclusions section

Scan exclusion is a set of conditions. When these conditions are met, Kaspersky Endpoint Security does not scan the objects for viruses and other malware. You can also exclude objects from scans by masks and threat names.

Settings of scan exclusions

Group of settings	Description
Exclusion scopes	This group of settings contains the **Configure** button. Clicking this button opens the Exclusion scopes window. In this window, you can define the list of scopes to be excluded from scans.
Exclusions by mask	This group of settings contains the **Configure** button, which opens the Exclusions by mask window. In this window, you can configure the exclusion of objects from scans by name mask.
Exclusions by threat name	This group of settings contains the **Configure** button, which opens the Exclusions by threat name window. In this window, you can configure the exclusion of objects from scans based on threat name.

Exclusion scopes window

This window contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table.

Exclusion scope settings

Setting	Description
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from scan.
Status	The status indicates whether the application uses this exclusion.

By default, the table of exclusion scopes is empty. You can add, edit, and delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

New exclusion scope window

In this window, you can add and configure scan exclusion scopes.

Exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the Exclusion scopes window. The entry field must not be blank.
Use this scope	The check box enables or disables exclusion of the scope from scan when the application is running. If this check box is selected, the application excludes this area during scans. If this check box is cleared, the application includes this area in the scan scope. You can later exclude this scope by selecting the check box. This check box is selected by default.
File system, access protocol, and path	The settings block lets you set the exclusion scope. In the drop-down list of file systems, you can select the type of file system of the directories to be excluded from scans: • **Local**, for local directories. • **Mounted** – mounted directories. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
	If **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom** – resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want add to the exclusion scope. You can use masks and tags to specify the path. The **/** path is specified by default. The application excludes all directories of the local file system from scan.

Setting	Description
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the exclusion scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks of the objects that the application excludes from scan. Masks are only applied to objects in the directory specified in the path field. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<id>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

Where:

`<id>` is the container ID.

`<name>` is a container name

`<path to local directory>` is the path to the local directory.

You can also use unique combinations of tags: `[container-id:<id>]`, `[container-name:<name>]`, `[image-id:<id>]`, and `[image-name:<name>]/path to local directory>`.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- `[container-name:<name>][image-name:<name>]/path to local directory>`
- `[container-id:<id>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<id>]/<path to local directory>`
- `[container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

Exclusions by mask window

You can configure scan exclusions for objects by name mask. The application will not scan files whose names contain the specified mask. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans.

Examples:
The `*.txt` mask refers to all text files.
The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

Exclusions by threat name window

You can configure the exclusion of objects from scans based on threat name. The application will not block the specified threats. By default, the list of threat names is empty.

You can add, edit, and delete threat names.

Container monitoring

In the Administration Console, you can configure the Container Monitoring component in the policy properties (**General settings** → **Container Scan settings**).

Container monitoring settings

Setting	Description
Enable namespace and container scan	This check box enables or disables the scanning of namespaces and containers in real time. This check box is selected by default.
Action with container upon threat detection	In the drop-down list, you can select the action to be performed on a container when an infected object is detected: • **Skip container**: if an infected object is detected, the application does not perform any action on the container. • **Stop container**: if an infected object is detected, the application stops the container. • **Stop container if disinfection fails** (default value) – the application stops the container if disinfection of the infected object fails. This setting is available when using the application under a license that supports this function.
Container Scan settings	The group of settings contains the **Configure** button. Clicking this button opens the Container Scan settings window.

Container Scan settings window

In this window, you can edit the settings for integrating Kaspersky Endpoint Security with the Docker container management system, the CRI-O environment, and the Podman and runc utilities.

Container Scan settings

Setting	Description
Use Docker	This check box enables or disables the use of the Docker container management system. This check box is selected by default.
Docker socket path	Entry field for the path or URI (Uniform Resource Identifier) of the Docker socket. Default value: /var/run/docker.sock.
Use CRI-O	The check box enables or disables the use of the CRI-O environment. This check box is selected by default.
File path	Entry field for the path to CRI-O configuration file. Default value: /etc/crio/crio.conf.
Use Podman	The check box enables or disables the use of the Podman utility. This check box is selected by default.
File path	Entry field for the path to the Podman utility executable file. Default value: /usr/bin/podman.
Root directory	Entry field for the path to the root directory of the container storage. Default value: /var/lib/containers/storage
Use runc	The check box enables or disables the use of the runc utility. This check box is selected by default.
File path	Entry field for the path to the runc utility executable file. Default value: /usr/bin/runc.
Root directory	Entry field for the path to the root directory of the container state storage. Default value: /run/runc.

Container Scan

In the Administration Console, you can scan containers and images using the *Container Scan* task.

You can create and run custom Container Scan tasks. You can manage scan settings by editing the settings of the tasks.

In the properties of the *Container Scan* task, in the **Settings** section, you can manage the settings listed in the table below.

Container Scan task settings

Setting	Description
Scan	This group of settings contains buttons that open windows where you can configure the Container Scan settings and general scan settings.
Actions on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Actions on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

In the properties of the *Container Scan* task, in the **Exclusions** section, you can also configure exclusions by mask and by threat name.

Container Scan settings window

In this window, you can configure container and image scan settings.

Container and image scan settings

Setting	Description
Scan containers	This check box enables or disables container scans. If the check box is selected, you can specify a name or a name mask for containers to be scanned. This check box is selected by default.
Name mask	Entry field for a name or a name mask for containers to be scanned. By default, the * mask is specified – all containers will be scanned.
Action on threat detection	In the drop-down list, you can select the action to be performed on a container when an infected object is detected: • **Skip container** – do not perform any actions on the container when an infected object is detected. • **Stop container** – stop container when an infected object is detected. • **Stop container if disinfection fails** (default value) – stop the container if disinfection of the infected object or elimination of the threat fails. Due to the way a CRI-O environment works, an infected object is not disinfected or deleted in a container in a CRI-O environment. We recommend selecting the **Stop container** action.
Scan images	This check box enables or disables the image scan. If the check box is selected, you can specify a name or a name mask for images to be scanned. This check box is selected by default.
Name mask	Entry field for a name or a name mask for images to be scanned. By default, the * mask is specified (all images are scanned).
Action on threat detection	In the drop-down list, you can select the action to be performed on an image when an infected object is detected: • **Skip image** (default value) – do not perform any actions on the image when an infected object is detected. • **Delete image** when an infected object is detected (not recommended). All dependencies will also be deleted. Running containers will be stopped, and then deleted.
Scan each layer	This check box enables or disables the scanning of all layers of images and running containers. This check box is cleared by default.

Scan settings window

In this window, you can configure the file scan settings for the task.

Setting	Description
Scan archives	This check box enables or disables scan of archives. If the check box is selected, the application scans the archives. To scan an archive, the application has to unpack it first, which may slow down scanning. You can reduce the duration of archive scans by configuring the **Skip file that is scanned for longer than (sec)** and **Skip file larger than (MB)** settings in the **General scan settings** section. If the check box is cleared, the application does not scan the archives. This check box is selected by default.
Scan SFX archives	This check box enables or disables *self-extracting archive* scans. Self-extracting archives are the archives that contain an executable extraction module. If the check box is selected, the application scans self-extracting archives. If the check box is cleared, the application does not scan self-extracting archives. This check box is available if the **Scan archives** check box is cleared. This check box is selected by default.
Scan mail databases	This check box enables or disables scans of mail databases of Microsoft Outlook, Outlook Express, The Bat!, and other mail applications. If the check box is selected, the application scans mail database files. If the check box is cleared, the application does not scan mail database files. This check box is cleared by default.
Scan mail format files	This check box enables or disables scan of files of plain-text email messages. If this check box is selected, the application scans plain-text messages. If this check box is cleared, the application does not scan plain-text messages. This check box is cleared by default.
Skip file that is scanned for longer than (sec)	In this field, you can specify the maximum time to scan a file, in seconds. After the specified time, the application stops scanning the file. Possible values: 0–9999. If the value is set to 0, the scan time is unlimited. Default value: 0.
Skip file larger than (MB)	In this field, you can specify the maximum size of a file to scan, in megabytes. Possible values: 0–999999. If the value is set to 0, the application scans files of any size. Default value: 0.
Log clean objects	This check box enables or disables the logging of *ObjectProcessed* type events. If this check box is selected, the application logs events of the *ObjectProcessed* type for all scanned objects. If this check box is cleared, the application does not log events of the *ObjectProcessed* type for any scanned object. This check box is cleared by default.
Log unprocessed objects	This check box enables or disables the logging *ObjectNotProcessed* type events if a file cannot be processed during a scan. If this check box is selected, the application logs the events of the *ObjectNotProcessed* type. If this check box is cleared, the application does not log the events of the *ObjectNotProcessed* type. This check box is cleared by default.
Log packed objects	This check box enables or disables the logging of *PackedObjectDetected* type events for all packed objects that are detected. If this check box is selected, the application logs the events of the *PackedObjectDetected* type. If this check box is cleared, the application does not log the events of the *PackedObjectDetected* type. This check box is cleared by default.
Use iChecker technology	This check box enables or disables scan of only new and modified since the last scan files. If the check box is selected, the application scans only new files or the files modified since the last scan. If the check box is cleared, the application scans the files regardless of the creation or modification date. This check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. This check box is selected by default.

Setting	Description
Heuristic analysis level	If the **Use heuristic analysis** check box is selected, you can select the heuristic analysis level in the drop-down list: • **Light** is the least detailed scan with minimal system load. • **Medium** is a medium scan with balanced system load. • **Deep** is the most detailed scan with maximum system load. • **Recommended** (default) is the optimal level recommended by Kaspersky experts. It ensures an optimal combination of protection quality and impact on the performance of the protected devices.
Do not run multiple scan tasks at the same time	Postponed start of scan tasks if a scan is already running. Kaspersky Endpoint Security will enqueue new scan tasks if the current scan continues. This helps optimize the load on the computer. For example, let's assume that the application has started a Full Scan task according to the schedule. If a user attempts to start a quick scan from the application interface, Kaspersky Endpoint Security will enqueue this quick scan task and then automatically start this task after the Full Scan task is finished. This check box is cleared by default.

Actions on threat detection window

In this window, you can configure actions to be performed by Kaspersky Endpoint Security on detected infected objects:

Actions on threat detection

Setting	Description
Actions on threat detection	You can select the action that the application performs on a detected infected object: • **Disinfect; delete if disinfection is not possible** (default). If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application deletes the infected object. • **Disinfect; inform if disinfection fails**. If you select this action, the application attempts to disinfect the infected object by saving a copy of the object in Backup. If disinfection is not possible (for example, if the type of object or the type of threat in the object cannot be disinfected), the application creates a record in the log. • **Inform**. If you select this action, the application creates a record about the infected object in the log.

Exclusions section

Settings of scan exclusions

Group of settings	Description
Exclusions by mask	This group of settings contains the **Configure** button, which opens the **Exclusions by mask** window. In this window, you can configure the exclusion of objects from scans by name mask.
Exclusions by threat name	This group of settings contains the **Configure** button, which opens the **Exclusions by threat name** window. In this window, you can configure the exclusion of objects from scans based on threat name.
Use global exclusions	The check box enables or disables the exclusion of the mount points specified in global exceptions while the application is running. If this check box is selected, the application excludes configured mount points from scans. This check box is selected by default.

Exclusions by mask window

You can configure scan exclusions for objects by name mask. The application will not scan files whose names contain the specified mask. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans.

Examples:
The `*.txt` mask refers to all text files.
The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

Exclusions by threat name window

You can configure the exclusion of objects from scans based on threat name. The application will not block the specified threats. By default, the list of threat names is empty.

You can add, edit, and delete threat names.

Removable drives scan

In the Administration Console, you can configure the settings for the removable drives scan in the policy properties (**Local Tasks** → **Removable Drives Scan**).

Removable Drives Scan component settings

Setting	Description
Enable removable drives scan when connected to the device	This check box enables or disables the scan of removable drives when they are connected to the user device. This check box is cleared by default.
Action when a removable drive connects	In the drop-down list, you can select an action to be performed by the application upon connection of removable drives to the user device: • **Do not scan** removable drives when connected (default value). • **Quick scan**: only scan files of certain types on removable drives (except CD/DVD drives and Blu-ray discs) and do not unpack compound objects. A quick scan is performed using the default settings for the *Critical Areas Scan* task. • **Detailed scan**: scan all files on removable drives (except CD/DVD drives and Blu-ray discs). A detailed scan is performed using the default settings for the *Malware Scan* task.
Action when a CD / DVD drive connects	In the drop-down list, you can select an action to be performed by the application upon connection of CD/DVD drives and Blu-ray discs to the user device: • **Do not scan** CD/DVD drives and Blu-ray discs when connected (default value). • **Quick scan**: only scans files of certain types on CD/DVD drives and Blu-ray discs. A quick scan is performed using the default settings for the *Critical Areas Scan* task. • **Detailed scan**: scan all files on CD/DVD drives and Blu-ray discs. A detailed scan is performed using the default settings for the *Malware Scan* task.
Block access to the removable drive while scanning	This check box enables or disables blocking of files on the connected drive during execution of the scan. This check box is cleared by default.

Useful articles

File types for quick scan

The following file formats are scanned on removable media: com, exe, sys, prg, bin, bat, cmd, dpl, dll, scr, cpl, ocx, tsp, drv, vxd, pif, lnk, reg, ini, cia, vbs, vbe, js, jse, htm, htt, hta, asp, chm, pht, wsh, wsf, the, hip, eml, nws, msg, pig, mbx, doc*, dot*, fpm, rtf, shs, dwg, msi, otm, pdf, swf, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx.

Behavior Detection

In the Administration Console, you can manage Behavior Detection settings in the policy properties (**Advanced Threat Protection** → **Behavior Detection**).

Behavior Detection component settings

Setting	Description
Enable Behavior Detection	This check box enables or disables the Behavior Detection component. This check box is selected by default.
Action on malware activity detection	The action to be performed by Kaspersky Endpoint Security upon detecting malicious activity in the operating system: • **Block** the application that performs malicious activity (default value). Kaspersky Endpoint Security terminates the process that performs malicious activity and logs information about the detected malicious activity. • **Inform** user. Kaspersky Endpoint Security does not terminate the process that performs malicious activity; it only records the detection of malicious activity in the event log.
Use exclusions by process	This check box enables or disables exclusions by process in the operation of the Behavior Detection component. This check box is cleared by default. The **Configure** button opens the **Exclusions by process** window. In this window, you can exclude the activity of processes.

Exclusions by process window

This window contains per-process exclusion scopes. The exclusion scope for exclusion by process lets you exclude the activity of an indicated process.

Exclusion scope settings for exclusion by process

Setting	Description
Merge inherited values	This check box enables or disables the merging of the list when inherited in child policies. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.
Exclusion scope name	Exclusion scope name.
Path	Full path to excluded process.
Status	The status indicates whether the application uses this exclusion.

By default, the table of exclusion scopes is empty. You can add, edit, or delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

Trusted process window

In this window, you can add and configure exclusion scopes for exclusion by process.

Exclusion scope settings for exclusion by process

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in a table in the Exclusions by process window.
Path to excluded process	Full path to the process you want to exclude from scans. You can use masks to specify the path. The entry field must not be blank.
Apply to child processes	Exclude child processes of the excluded process indicated by the **Path to excluded process** setting. This check box is cleared by default.
Use this scope	The check box enables or disables this exclusion scope. If this check box is selected, the application excludes this scope. If this check box is cleared, the application includes this scope. You can later exclude this scope by selecting the check box. This check box is selected by default.
Exclude process from Behavior Detection scans	This check box enables or disables the exclusion of the process from scanning by Behavior Detection. This check box is cleared by default.
Exclude process from MDR and EDR Expert (on-premises) telemetry	This check box enables or disables the exclusion of the process from telemetry collected by the MDR and EDR Expert (on-premises) components. This check box is cleared by default.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Exploit Prevention

In the Administration Console, you can configure Exploit Prevention in the policy properties (**Advanced Threat Protection → Behavior Detection**).

Exploit Prevention component settings

Setting	Description
Enable Exploit Prevention	This check box enables or disables Exploit Prevention. This check box is cleared by default.
Exploit Prevention	Clicking the **Configure** button opens the Exploit Prevention exclusions window, in which you can configure exclusions from scanning for the Exploit Prevention component.

Setting	Description
Action on exploit detection	The action that the application will perform when an exploit is detected: • **Block** (default value). The application blocks the malicious activity of the exploit and records information about this in the event log. • **Inform**. The application does not block the activity of the exploit, but only records information about exploit detection in the event log.

Exploit Prevention exclusions window

In this window, you can configure the exclusion of objects from Exploit Prevention scans. The application will not scan the specified objects. By default, the list of objects is empty.

Exploit Prevention exclusion settings

Setting	Description
Merge inherited values	This check box enables or disables the merging of the list when inherited in child policies. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.
Status	The status indicates whether the application uses this exclusion.
Threat name.	Name of the threat to be excluded from scanning.
File or directory path	Full path to the file or directory excluded from scanning.
File hash	Hash of the file excluded from scanning.
Comment	Comment for the scan exclusion.

By default, the table of exclusions is empty. You can add, edit, or delete items in the table.

Exploit Prevention exclusion window

In this window, you can add or configure an exclusion for objects from Exploit Prevention scans.

Exploit Prevention exclusion settings

Setting	Description
Use threat name	This check box enables or disables the exclusion from scanning by the name of the threat detected in the object. This check box is selected by default.
Threat name.	In this field, you can enter the name of the threat detected in the object. In order to exclude an object from scans, specify the full name of the threat detected in this object – the string containing the application's decision that the object is infected. You can find the full name of the threat detected in an object in the application log or on the website https://threats.kaspersky.com. This field is available if the **Use threat name** check box is selected.
Use file hash	This check box enables or disables the exclusion from scanning by file hash. This check box is selected by default.
File hash sum type	In this drop-down list, you can select the type of file hash that you want to use to exclude the file from scanning: • **MD5**. • **SHA256**. This drop-down list is available if the **Use file hash** check box is selected.
File hash sum	In this field, you can entering the hash of the file by which you want to exclude the file from scanning. This field is available if the **Use file hash** check box is selected.
Use file or directory path	This check box enables or disables the exclusion of files in which a threat is detected by their paths. This check box is selected by default.

Setting	Description
File or directory path	Entry field for specifying the path to the file or directory that you want to exclude from a scan. You can use the * and ? characters in the path. The field is available if the **Use file or directory path** check box is selected.
Comment	Entry field for a comment (optional).
Use this exclusion	This check box enables or disables the use of this exclusion when the application is running. This check box is selected by default.

Anti-Cryptor

In the Administration Console, you can manage Anti-Cryptor settings in the policy properties (**Advanced Threat Protection → Anti-Cryptor**).

Anti-Cryptor component settings

Setting	Description
Enable Anti-Cryptor	This check box enables or disables the protection of files in local directories with network access by SMB/NFS protocols from remote malicious encryption. This check box is cleared by default.
Protection scopes	This group of settings contains buttons that open windows where you can configure the scan scopes and protection settings.
Exclusions	This group of settings contains the **Configure** button. Clicking this button opens the **Exclusion scopes** window. In this window, you can define the list of scopes to be excluded from scans.
Exclusions by mask	This group of settings contains the **Configure** button, which opens the **Exclusions by mask** window. In this window, you can configure the exclusion of objects from scans by name mask.

Scan scopes window

The table contains the scan scopes. The application will scan files and directories located in the paths specified in the table. By default, the table contains one scan scope that includes all directories of the local file system.

Scan scope settings

Setting	Description
Scope name	Scan scope name.
Path	Path to the directory that the application scans.
Status	The status indicates whether the application scans this scope.

You can **add**, **edit**, **delete**, **move up**, and **move down** items in the table.

Clicking the **Move down** button moves the selected item down in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they are listed in the table of scan scopes. If you want to configure security settings for a subdirectory that are different from the security settings of the parent directory, you must place the subdirectory higher than its parent directory in the table.

This button is available if a scope is selected in the table.

Clicking the **Delete** button excludes the selected scope from scans.

This button is available if at least one scan scope is selected in the table.

The selected element's settings are changed in a separate window.

Clicking the **Add** button opens a window where you can specify the new item settings.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

New scan scope window

In this window, you can add or configure protection scope for the Anti-Cryptor component.

Protection scope settings

Setting	Description
Scope name	Field for entering the protection scope name. This name will be displayed in the table in the Scan scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables scans of this scope by the application. If this check box is selected, the application processes this protection scope during the component operation. If this check box is cleared, the application does not process this protection scope during the component operation. You can later include this scope in the component operation settings by selecting the check box. This check box is selected by default.
File system, access protocol, and path	The settings block lets you set the scan scope. You can select the file system type in the drop-down list of file systems: • **Local**, for local directories. • **Shared** displays server file system resources accessible via the Samba or NFS protocol. • **All shared** (default value) displays all server file system resources accessible via the Samba and NFS protocols.
	If **Shared** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want to add to the protection scope. You can use masks to specify the path. The field must not be blank.
Masks	This list contains name masks of the objects that the application scans during operation of the Anti-Cryptor component. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the * (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Protection settings window

Protection settings

Setting	Description
Action on encryption detection	The action to be performed by Kaspersky Endpoint Security upon detecting malicious encryption: • **Inform** user. Kaspersky Endpoint Security does not block the device performing encryption; it only records in the event log an event about the detection of malicious encryption. • **Block** the device performing encryption (default value).
Block untrusted host for (min)	In this field you can specify the untrusted host blocking duration in minutes. After the specified time, Kaspersky Endpoint Security removes the untrusted devices from the list of blocked devices. The access of the host to network file resources is restored automatically, after it is deleted from the list of untrusted hosts. If a compromised host is blocked and you change this setting value, the blocking time for this host will not change. The blocking time is not a dynamic value, and it is calculated at the moment of blocking. Possible values: integers from 1 to 2147483647. Default value: 30.

Exclusion scopes window

This window contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table.

Exclusion scope settings

Setting	Description
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from scan.
Status	The status indicates whether the application uses this exclusion.

By default, the table of exclusion scopes is empty. You can add, edit, and delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

New exclusion scope window

- In this window, you can add and configure scan exclusion scopes.

Exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the **Exclusion scopes** window. The entry field must not be blank.
Use this scope	The check box enables or disables exclusion of the scope from scan when the application is running. If this check box is selected, the application excludes this area during scans. If this check box is cleared, the application includes this area in the scan scope. You can later exclude this scope by selecting the check box. This check box is selected by default.
File system, access protocol, and path	The settings block lets you set the exclusion scope. In the drop-down list of file systems, you can select the type of file system of the directories to be excluded from scans: • **Local** for local directories. • **Mounted** for mounted directories. • **All remote mounted** for all remote directories mounted on the device using the Samba and NFS protocols.
	If **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS** for remote directories mounted on the device using the NFS protocol. • **Samba** for remote directories mounted on the device using the Samba protocol. • **Custom** for resources of the device's file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a directory that you want add to the exclusion scope. You can use masks and tags to specify the path. The **/** path is specified by default. The application excludes all directories of the local file system from scan.
Filesystem name	The field for entering the name of the file system where the directories that you want to add to the exclusion scope are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.
Masks	The list contains name masks of the objects that the application excludes from scan. Masks are only applied to objects in the directory specified in the path field. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

How to use tags

You can use special tags to specify a container or image:

- `[container-id:<id>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`

- [image-id:<id>]/<path to local directory>
- [image-name:<name>]/<path to local directory>

Where:

<id> is the container ID.

<name> is a container name

<path to local directory> is the path to the local directory.

You can also use unique combinations of tags: [container-id:<id>], [container-name:<name>], [image-id:<id>], and [image-name:<name>]/path to local directory>.

Any combination of 1 to 4 unique tags within one area is allowed. The order they are listed in is not important.

For example:

- [container-name:<name>][image-name:<name>]/path to local directory>
- [container-id:<id>][image-name:<name>]/<path to local directory>
- [image-name:<name>][image-id:<id>]/<path to local directory>
- [container-name:<name>][container-id:<id>][image-name:<name>]/<path to local directory>
- [container-name:<name>][image-id:<id>][container-id:<id>][image-name:<name>]/path to local directory>

You can use masks (? and * characters) in names and identifiers.

Exclusions by mask window

You can configure scan exclusions for objects by name mask. The application will not scan files whose names contain the specified mask. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans.

Examples:
The *.txt mask refers to all text files.
The *_my_file_??.html mask refers to html files starting with any characters, and ending with _my_file_ followed by any two characters (for example, 2020_my_file_09.html).

You can enable the merging of the list of exclusions when inherited by child policies. If you want to merge list items, select the **Merge inherited values** check box. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.

Kaspersky Security Network

In the Administration Console, you can configure the use of Kaspersky Security Network in Kaspersky Endpoint Security in the policy properties (**Advanced Threat Protection** → **Kaspersky Security Network**).

You can read the text of the **Kaspersky Security Network Statement** in the Kaspersky Security Network Statement window, which can be opened by clicking the **Kaspersky Security Network Statement** link.

Kaspersky Security Center displays information about the availability of KSN via the client device status (*OK, Critical, Warning*) in the list of managed devices on the **Devices** tab.

Kaspersky Security Network settings

Setting	Description
Kaspersky Security Network Statement	Clicking this link opens the **Kaspersky Security Network Statement** window. In this window, you can read the text of the Kaspersky Security Network Statement.
Kaspersky Security Network (KSN)	This block displays information about the KSN mode or indicates that KSN is not used by Kaspersky Endpoint Security. The **Edit** button opens a window where you can configure the use of Kaspersky Security Network.
Enable cloud mode	In *cloud mode*, Kaspersky Endpoint Security uses a lightweight version of the anti-virus databases, which about halves the load on the RAM of the computer. The check box is available if use of KSN is enabled. The check box is selected if, when creating a policy, you accepted the terms of the Kaspersky Security Network Statement and are using KSN in extended mode. The mode is enabled or disabled after the next application database update. This setting applies only if the application is used in standard mode.
Use Administration Server as a KSN proxy server	If this check box is selected, Kaspersky Endpoint Security communicates with KSN servers using the KSN Proxy service on the Administration Server. This check box is selected by default. This setting applies only if the application is used in standard mode. In Light Agent mode, the application can only communicate with the KSN infrastructure through a KSN proxy server.
Use KSN servers when KSN Proxy is not available	If this check box is selected, Kaspersky Endpoint Security communicates with KSN servers directly when the KSN Proxy service is unavailable. This check box is selected by default. This check box is available if the **Use Administration Server as a KSN proxy server** check box is selected. This setting applies only if the application is used in standard mode.

Kaspersky Security Network settings

In this window, you can configure Kaspersky Security Network participation settings.

Kaspersky Security Network settings

Setting	Description
More info	Clicking this link opens the Kaspersky website.
Do not use Kaspersky Security Network	By selecting this option, you decline to use Kaspersky Security Network.
Basic KSN mode	By selecting this option, you accept the terms of using Kaspersky Security Network. You will be able to receive information from Kaspersky's online knowledge base about the reputation of files, web resources, and software.
Extended KSN mode	By selecting this option, you accept the terms of using Kaspersky Security Network. You will be able to receive information from Kaspersky's online knowledge base about the reputation of files, web resources, and software. Also, anonymous statistics and information about the types and sources of various threats will be sent to Kaspersky to improve Kaspersky Security Network.
Kaspersky Security Network Statement	This link opens the Kaspersky Security Network Statement window, where you can read the text of the Kaspersky Security Network Statement.

Kaspersky Security Network Statement

In this window, you can read the text of the Kaspersky Security Network Statement and accept its terms and conditions.

Kaspersky Security Network settings

Setting	Description
I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement	By selecting this option, you confirm that you want to use the Kaspersky Security Network, and you have fully read, understood, and accept the terms and conditions of the Kaspersky Security Network Statement that is displayed. This option is available if you selected the **Basic KSN mode** or **Extended KSN mode** option in the Kaspersky Security Network settings window.
I do not accept the terms and conditions of the Kaspersky Security Network Statement	By selecting this option, you confirm that you do not want to use Kaspersky Security Network. This option is available if you selected the **Basic KSN mode** or **Extended KSN mode** option in the Kaspersky Security Network settings window.

Kaspersky Private Security Network Statement

In this window, you can read the text of the Kaspersky Private Security Network Statement and accept its terms and conditions.

Kaspersky Security Network settings

Setting	Description
I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement	By selecting this option, you confirm that you want to participate in the Kaspersky Security Network, and you have fully read, understood, and accept the terms and conditions of the Kaspersky Private Security Network Statement that is displayed.
I do not accept the terms and conditions of the Kaspersky Security Network Statement	By selecting this option, you confirm that you do not want to use Kaspersky Security Network.

BadUSB Attack Prevention

In the Administration Console, you can manage Web Threat Protection settings in the policy properties (**Essential Threat Protection → BadUSB Attack Prevention**).

BadUSB Attack Prevention component settings

Setting	Description
Enable BadUSB Attack Prevention	This check box enables or disables the BadUSB Attack Prevention component. The component is disabled by default.
Maximum number of USB device authorization attempts	Automatically block the USB device if the authorization code is entered incorrectly the specified number of times. Valid values are 1 to 10. For example, if you allow five attempts to enter the authorization code, the application blocks the USB device after the fifth unsuccessful attempt. Kaspersky Endpoint Security displays the time for which the USB device is blocked. After this time elapses, you will once again have five attempts to enter the authorization code.
Blocking duration when the maximum number of authorization attempts is reached (minutes)	USB device block duration after the specified number of unsuccessful attempts to enter the authorization code. Possible values: 1 to 180 (minutes)
Do not allow using an on-screen keyboard when authorizing USB devices	If the toggle button is switched on, the application blocks use of On-Screen Keyboard for authorization of a USB device from which an authorization code cannot be entered.
Prohibit use of a barcode for authorization of USB devices	If this toggle switch is enabled, the application does not allow to use a barcode for authorization of a USB device that cannot be used to enter an authorization code.

Communication & Web Protection

Mail Threat Protection

In the Administration Console, you can manage Web Threat Protection settings in the policy properties (**Essential Threat Protection → Mail Threat Protection**).

Mail Threat Protection component settings

Setting	Description
Mail Threat Protection	This check box enables or disables Mail Threat Protection. This component is enabled by default.
Configure (Protection settings)	Clicking this button opens the **Mail Threat Protection settings** window, in which you can configure the Mail Threat Protection scope and the scan settings for compound files.
Configure (Attachment filter)	Clicking this button opens the **Attachment filter** window, in which you can configure the filtering of email attachments.
Use the heuristic analyzer **Heuristic analysis level**	This check box enables or disables the use of the heuristic analyzer. When scanning files for malicious code, the heuristic analyzer executes instructions in executable files. How many instructions the heuristic analyzer executes depends on the specified heuristic analysis level. The heuristic analysis level sets the balance between the thoroughness of searches for novel threats, the load on the operating system's resources, and the duration of heuristic analysis. By default, the heuristic analyzer is enabled and the medium heuristic analysis level is selected.

Setting	Description
Actions on threat detection	The action that Mail Threat Protection performs when a threat is detected in email messages: • **Disinfect; delete if disinfection is not possible**. When an infected object is detected in an incoming message, the application attempts to disinfect the detected object. The message with the safe attachment is then made available to the user. If disinfection fails, the application deletes the infected object. The application adds information about the performed action to the message subject, for example, *[The message has been processed] <message subject>*. This action is selected by default. • **Disinfect; block if disinfection fails**. When an infected object is detected in an incoming message, the application attempts to disinfect the detected object. The message with the safe attachment is then made available to the user. If disinfection fails, the application adds a warning to the subject of the message. The message with the original attachment is then made available to the user. • **Block**. If an infected object is detected in an incoming message, the application adds a warning to the message subject. The message with the original attachment is then made available to the user. This setting is not applicable to outgoing messages. If an infected object is detected in an outgoing message, the application blocks the message from being sent.

Mail Threat Protection settings window

In this window, you can configure the Mail Threat Protection scope and compound file scan settings.

Mail Threat Protection settings

Setting	Description
Protection scope	The *protection scope* specifies which objects the component must scan: incoming and outgoing messages or only incoming messages. By default, the **Incoming and outgoing messages** option is selected.
Scan archive attachments	Enables or disables the scanning of attached archives. This includes the scanning of ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE and other types of archives. The application identifies archives not just by extension, but also by format. When scanning archives, the application performs recursive unpacking. This makes it possible to detect threats in nested archives (archive inside an archive). This check box is selected by default.
Scan attached office application files	Enables or disables the scanning of attached files in office formats. The application scans office-format attachments smaller than 1 MB regardless of the state of whether this check box is selected or not. This check box is selected by default.
Do not scan archives larger than (MB)	If this check box is selected, Mail Threat Protection excludes from scanning any attached archives that are larger than the specified limit. If this check box is cleared, Mail Threat Protection scans attached archives of any size. This check box is cleared by default.
Limit archive scan duration to (seconds)	If this check box is selected, the scan duration for archives attached to email messages is limited. This check box is cleared by default.

Attachment filter window

In this window, you can configure email attachment filtering.

Attachment filtering settings

Setting	Description
Do not apply filter	If this option is selected, Mail Threat Protection does not filter files attached to email messages.
Rename attachments of specified types	If this option is selected, Mail Threat Protection replaces the last character of the extension with an underscore character for specified file types (for example, attachment.doc_). Thus, to open the file, the user needs to rename the file. Selected by default.
Delete attachments of specified types	If this option is selected, Mail Threat Protection deletes attachments of the specified types from email messages. You can specify the types of attachments to rename or delete from email messages in the list of file masks.

Setting	Description
Merge inherited values	This check box enables or disables the merging of the list when inherited in child policies. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.
Table of attachment types	This table lists the types of attachments that you want to rename or delete from email messages. You can add, edit, or remove attachment types using the corresponding buttons.

Web Threat Protection

In the Administration Console, you can configure Web Threat Protection settings in the policy properties (**Essential Threat Protection → Web Threat Protection**).

Web Threat Protection component settings

Setting	Description
Enable Web Threat Protection	This check box enables or disables Web Threat Protection. This check box is cleared by default.
Trusted web addresses	This group of settings contains the **Configure** button, which opens the **Trusted web addresses** window, where you can specify the list of trusted web addresses. The application will not scan the contents of websites whose web addresses are included in this list.
Action on threat detection	Action that the application performs on a web resource where a dangerous object is detected: • **Block** access to all dangerous objects detected in web traffic, display a notification about the blocked access attempts, and log information about the dangerous objects (default value). • **Inform** the user when a dangerous object is detected in web traffic. Web Threat Protection allows this object to be downloaded to the device. At that, the application logs the information about the dangerous object and adds it to the list of active threats.
Scan settings	This group of settings contains the **Configure** button, which opens the **Scan settings** window, where you can configure the settings for scanning incoming traffic.

Trusted web addresses window

In this window, you can add web addresses and web pages whose content you consider trusted.

You can only add HTTP/HTTPS web addresses to the list of trusted web addresses. You can use masks to specify web addresses. Masks are not supported to specify IP addresses. By default, the list is empty. You can add, edit, and remove web addresses on the list.

Useful articles

How to specify masks

When creating an address mask, use an asterisk (*) as a placeholder for one or more characters. If you enter the *abc* address mask, it is applied to all web resources that contain the "abc" sequence (for example, www.virus.com/download_virus/page_0-9abcdef.html). To include the asterisk in the address mask as a character, but not as a mask, enter the * character twice (for example, www.virus.com/**/page_0-9abcdef.html means www.virus.com/*/page_0-9abcdef.html).

Scan settings window

In this window, you can configure the settings for scanning incoming traffic during operation of the Web Threat Protection component.

Web Threat Protection settings

Setting	Description
Detect malicious objects	This check box enables or disables checking of links against the databases of malicious web addresses. This check box is selected by default.
Detect phishing links	This check box enables or disables checking of links against the databases of phishing web addresses. This check box is selected by default.
Use heuristic analysis for detecting phishing links	This check box enables or disables the use of heuristic analysis for detecting phishing links. This check box is available if the **Detect phishing links** check box is selected, and is selected by default.
Detect adware	This check box enables or disables checking links against the databases of adware web addresses. This check box is cleared by default.
Detect legitimate applications that intruders can use to compromise devices or data	This check box enables or disables checking links against the databases of legitimate applications that intruders can use to compromise devices or data. This check box is cleared by default.

Network Threat Protection

In the Administration Console, you can manage Network Threat Protection settings in the policy properties (**Essential Threat Protection** → **Network Threat Protection**).

Network Threat Protection component settings

Setting	Description
Enable Network Threat Protection	This check box enables or disables Network Threat Protection. This check box is cleared by default.
Action on threat detection	Actions performed upon detection of network activity that is typical of network attacks. • **Inform** user. The application allows network activity and logs information about detected network activity. • **Block** network activity from an attacking device and log information about detected network activity (default value).
Block attacking devices	This check box enables or disables the blocking of network activity when a network attack attempt is detected. This check box is selected by default.
Block the attacking device for (min)	In this field you can specify the duration an attacking device is blocked in minutes. After the specified time, Kaspersky Endpoint Security allows network activity from this device. Possible values: integers from 1 to 32768. Default value: 60.
Exclusions	This group of settings contains the **Configure** button, which opens the Exclusions window, where you can specify a list of IP addresses. Network attacks from these IP addresses will not be blocked.

Exclusions window

In this window, you can add IP addresses from which network attacks will not be blocked.

By default, the list is empty.

You can add, edit, and remove IP addresses in the list. You can specify IP addresses in IPv4 and IPv6 formats.

Firewall Management

In the Administration Console, you can configure Firewall Management settings in the policy properties (**Essential Threat Protection** → **Firewall Management**).

Firewall Management settings

Setting	Description
Enable Firewall Management	This check box enables or disables Firewall Management. This check box is cleared by default.
Network packet rules	This group of settings contains the **Configure** button. Clicking this button opens the Network packet rules window. In this window, you can configure network packet rules that are applied by the Firewall Management component when it detects the network connection attempt.
Available networks	This group of settings contains the **Configure** button. Clicking this button opens the Available networks window. In this window, you can configure the list of networks that the Firewall Management component will monitor.
Incoming connections	In this drop-down list, you can select the action to be performed for incoming network connections: • **Allow** network connections (default value). • **Block** network connections.
Incoming packets	In this drop-down list you can select the action to be performed for incoming packets: • **Allow** incoming packets (default value). • **Block** incoming packets.
Always add allowing rules for Network Agent ports	This check box enables or disables the automatic adding of allowing rules for Network Agent ports. This check box is selected by default.

Network packet rules window

The **Network packet rules** table contains network packet rules that the Firewall Management component uses for network activity monitoring. You can configure the settings described in the table below for network packet rules.

Network packet rules settings

Setting	Description
Name	Network packet rule name.
Action	Action to be performed by Firewall Management when it detects the network activity.
Local address	Network addresses of devices that have Kaspersky Endpoint Security installed and can send and/or receive network packets.
Remote address	Network addresses of remote devices that can send and/or receive network packets.
Logging	This column shows if the application logs actions of the network packet rule. If the value is **Yes**, the application logs the actions of the network packet rule. If the value is **No**, the application does not log the actions of the network packet rule.

By default, the table of network packet rules is empty.

You can add, edit, delete, move up, and move down network packet rules in the table.

Added network packet rule window

In this window, you can configure the added network packet rule settings.

Network packet rule settings

Setting	Description
Protocol	You can select the type of data transfer protocol for which you want to monitor network activity: • **Any** (default value) • **GRE** • **ICMP** • **ICMPv6** • **IGMP** • **TCP** • **UDP**
Direction	You can specify the direction of network activity being monitored: • **Incoming packets**. If this option is selected, the Firewall Management component monitors only incoming packets. • **Incoming**. If this option is selected, the Firewall Management component monitors only incoming connections. • **Incoming/Outgoing** (default setting). If this option is selected, the Firewall Management component monitors both incoming and outgoing connections. • **Incoming/Outgoing packets**. If this option is selected, the Firewall Management component monitors both incoming and outgoing packets. • **Outgoing packets**. If this option is selected, the Firewall Management component monitors only outgoing packets. • **Outgoing**. If this option is selected, the Firewall Management component monitors only outgoing connections.
ICMP type	You can specify the ICMP type. The Firewall Management component monitors messages of the specified type sent by the host or gateway. If the **Specified** option is selected, the field for entering the ICMP type will be displayed. This window is displayed if the **ICMP** or **ICMPv6** data transfer protocol is selected in the **Protocol** drop-down list.
ICMP code	You can specify the ICMP code. The Firewall Management component monitors messages of the type specified in the **ICMP type** field, with the code specified in the **ICMP code** field, and sent by the host or gateway. If the **Specified** option is selected, the field for entering the ICMP code will be displayed. This window is displayed if the **ICMP** or **ICMPv6** data transfer protocol is selected in the **Protocol** drop-down list.
Remote ports	You can specify a port number or port range of the remote devices between which the connection is to be monitored. If the **Specified** option is selected, the field for entering the port numbers will be displayed. This window is displayed only if **TCP** or **UDP** data transfer protocol is selected in the **Protocol** drop-down list.
Local ports	You can specify a port number or port range of the local devices between which the connection is to be monitored. If the **Specified** option is selected, the field for entering the port numbers will be displayed. This window is displayed only if **TCP** or **UDP** data transfer protocol is selected in the **Protocol** drop-down list.
Remote addresses	You can specify the network addresses of the remote devices that can send and receive network packets: • **Any address** (default value). If this item is selected, the network rule controls network packets sent and/or received by remote devices with any IP address. • **Specified address or address range**. If this option is selected, the network rule controls the sending and receiving of network packets by remote devices with the IP addresses that are specified in the table below. Clicking the **Add** button above the table opens the Add IP addresses window, in which you can specify an IP address of the device, a network address, or a range of IP addresses. • **By network type**. If this item is selected, the network rule controls network packets sent and received by remote devices with the IP addresses associated with the selected network type: **Public networks**, **Local networks**, or **Trusted networks**.
Local addresses	You can specify the network addresses of the devices with Kaspersky Endpoint Security installed that can send and receive network packets: • **Any address** (default value). If this option is selected, the network rule controls network packets sent and/or received by the devices with Kaspersky Endpoint Security installed regardless of their IP address. • **Specified address or address range**. If this option is selected, the network rule controls the network addresses of devices with Kaspersky Endpoint Security installed that can send and receive network packets. These network addresses are specified in the table below. Clicking the **Add** button above the table opens the Add IP addresses window, in which you can specify an IP address of the device, a network address, or a range of IP addresses.
Action	You can select an action to be performed by the Firewall Management component when it detects network activity: • **Block** network activity. • **Allow** network activity (default value).
Logging	You can specify whether the actions of the network rule will be logged in the report.
Rule name	The field for entering the name of the network packet rule.

Add IP addresses window

In this window, you can specify the IP address of the device, network address or range of IP addresses.

You can specify multiple addresses; enter each address on a new line for convenience of copying them.

Available networks window

The **Available networks** table contains the networks controlled by the Firewall Management component. The table of available networks is empty by default.

Available networks settings

Setting	Description
IP address	Network IP address.
Network type	Network type (**Public network**, **Local network**, or **Trusted network**).

You can add, edit, and delete available networks.

Network connection window

In this window, you can configure the network connection that the Firewall Management component will monitor.

Network connection

Setting	Description
IP address	The field for entering IP address of the network.
Network type	You can select the type of the network: • **Public** • **Local** • **Trusted**

Security Controls

Device Control

In the Administration Console, you can manage Device Control settings in the policy properties (**Security Controls** → **Device Control**).

Device Control settings

Setting	Description
Enable Device Control	This check box enables or disables Device Control. This check box is selected by default.
Trusted devices	This group of settings contains the **Configure** button. Clicking this button opens the Trusted devices window. In this window, you can add a device to the list of trusted devices.
Device Control operating mode	Response to attempts to access a device that is restricted according to Device Control rules: • **Inform**. If you select this option, Kaspersky Endpoint Security tests the selected access mode and generates an event for the detected attempt to access a device. • **Block** (default value). If you select this option, Kaspersky Endpoint Security applies the access mode set for the device or bus.
Device Control settings	This group of settings contains buttons that open windows where you can configure access mode for devices by type and connection buses.

Setting	Description
Allow requesting temporary access	If this check box is selected, the user can request temporary access to the blocked device in the graphical interface of the application or on the command line.
Message templates	This group of settings contains the **Configure** button. Clicking this button opens the **Message templates** window.

Trusted devices window

The table contains a list of trusted devices. The table is empty by default.

Trusted device settings

Setting	Description
Device ID	ID of a trusted device.
Device name	Trusted device name.
Device type	Trusted device type (for example, Hard drive or Smart card reader).
Host name	Name of the client device the trusted device is connected to.
User or group name	Name of the user or group for which the device is trusted.
Comment	Comment related to a trusted device.

You can add devices to the trusted device list using the **Add** button as follows:

- Specify a device ID or device ID mask (**Add** → **Add device by ID or mask**).
- Select the desired device from the list of devices detected on managed devices (**Add** → **Select a device from the list of devices detected on hosts**).
- Select the desired device from the list of devices detected in Device Control events in Kaspersky Security Center (**Add** → **Add device based on events**).

You can edit and delete trusted devices in the table.

You can also export the list of added devices to a file by clicking the **Advanced** → **Export selected** or **Advanced** → **Export all** button and import a list of devices from a JSON file by clicking the **Advanced** → **Import** button.

Three import modes are possible:

- **Combine with existing** to merge the lists of trusted devices upon import. If the file already has an entry for this device ID, settings of the existing entry are updated. For devices that were not previously on the list, entries are added.
- **Add to existing** to add trusted devices to the list upon import. Only entries for devices not previously on the list of devices are added to the list.
- **Replace existing** to replace the list of trusted devices. The existing list of trusted devices is replaced with the list from the file.

Trusted device (Device ID) window

In this window, you can add a device to the list of trusted devices by its identifier.

Adding device by ID

Setting	Description
Device ID	The field for entering the identifier or the identifier mask of the device that you want to add to the list of trusted devices. To specify an identifier, you can use the following wildcards: * (any sequence of characters) or ? (any single character). For example, you can specify the USBSTOR* mask to allow access to all USB drives.
Find on hosts	Clicking the button displays the devices found on the connected client devices using the specified ID or mask. The button is available if the **Device ID** field is not empty.
Devices found	The table contains the following columns: • **Device type** – type of device found (for example, Hard drive or Smart card reader). • **Device ID** – ID of the device found. • **Device name** – name of the device found. • **Host name** — name of the client device that the found device is connected to.
Comment	The field for entering a comment for the device that you want to add to the list of trusted devices (optional).
Allow access for users and/or groups of users	This field displays the name of the user and/or group for which the device is trusted. The default value is **\Everyone** (all users).
Configure	Clicking the button opens the Access to trusted device window.

Device window on client devices

In this window you can add a device to the list of trusted devices by selecting it in the list of existing managed devices.

Information about existing devices is available only if an active policy has been created and synchronization with the Network Agent has been performed (the synchronization interval is specified in the Network Agent policy, 15 minutes by default).

When you create a new inactive policy, the list will be empty.

Adding a device from the list of devices detected on managed client devices

Setting	Description
Host name	Field for entering the name or the name mask for the managed device for which you want to find connected devices. The default mask is * – all managed devices.
Device type	In this drop-down list, you can select the type of connected device to search for (for example, Hard drives or Smart card readers). The **All devices** option is selected by default.
Device ID	Field for entering the identifier or identifier mask for the device you want to find. The default mask is * – all devices.
Find on hosts	When you click this button, the application searches for devices with the specified parameters. The search results are displayed in the table below.
List of detected devices	The table contains the following columns: • **Host name** — name of the client device that the found device is connected to. • **Device type** – type of device found (for example, Hard drive or Smart card reader). • **Device name** – name of the device found. • **Device ID** – ID of the device found.

List of devices based on Device Control events window

In this window, you can create a list of devices detected in Device Control events in Kaspersky Security Center. You can then add devices from this list to the list of trusted devices.

You can select one or more devices to add to the list of trusted devices.

Information about devices is available if Device Control is enabled, there is an active policy, and synchronization with Network Agent has been performed (synchronization is performed at the frequency specified in the Network Agent policy; by default – every 15 minutes).

When you create a new inactive policy, the list will be empty.

Adding devices from the list of devices detected in Kaspersky Security Center events

Setting	Description
Event types	You can use check boxes to select the types of Device Control events sent to Kaspersky Security Center. The list includes the devices detected in events of the specified types. All check boxes are selected by default.
Administration group	A field for entering the name of the administration group containing the client devices that the detected devices are connected to. Only devices connected to client devices from the specified administration group are included in the list. You can specify part of the group name. By default, the list includes devices connected to client devices in any administration group.
Events from period	In the drop-down list, you can select the time period when the events occurred. The list includes devices that were detected in events sent to Kaspersky Security Center during the specified period. By default, the list includes devices detected in events over the last month.
Search for devices	When you click this button, the application searches for devices with the specified parameters. The search results are displayed in the table below.
Devices found	The table contains the following columns: • **Device type** – type of device found (for example, Hard drive or Smart card reader). • **Device ID** – ID of the device found. • **Device name** – name of the device found. • **Host name** — name of the client device that the found device is connected to. • **Connection date** is the date when the found device was connected. • **Administration group** is the name of the administration group containing the client device that the detected device is connected to.
Comment	The field for entering a comment for the device that you want to add to the list of trusted devices (optional).
Allow access for users and/or groups of users	This field displays the name of the user and/or group for which the device is trusted. The default value is **\Everyone** (all users).
Configure	Clicking the button opens the **Access to trusted device** window.

Access to trusted device window

In this window, you can configure access of users or user groups to a selected trusted device.

Access to trusted device

Setting	Description
Users and/or user groups	List of users and groups for which you want to make the added device trusted. By default, the table contains the **\Everyone** item (all users). You can add, edit, or delete users or user groups.

User or group window

In this window, you can specify a user or a user group for which you want to make the device trusted.

Trusted device settings

Setting	Description
Type	The **user** or **group** for which you want to make the device trusted.
User or group name	Name of a local or domain user (without specifying the full name with the domain, if the system allows entering user names in this format, or in the `<domain name>\<user name>` or `<user name>@<domain name>`) format, or the name of a group of users for which you want to make the device trusted.

Device type window

In this window, you can configure access mode for various types of devices.

Access mode for device types

Setting	Description
Device type	Device type (for example, Hard drives, Printers).
Access mode	Device access mode. Right-clicking with the mouse opens a context menu where you can select one of the following items: • **Allow**: allow access to devices of the selected type. • **Block**: prohibit access to devices of the selected type. • **Depends on bus** (default value): allow or block access to the devices depending on the access mode for a connection bus. • **By rule**: allow or block access to devices depending on the access rule and schedule. This menu command is available only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives). • **Read only**: allow read-only access to devices of the selected type. This menu command is available only for storage devices (hard drives, removable drives, floppy disk drives, CD/DVD drives).

You can configure access rules and schedules in the **Configure device access rule** window, which opens when you double-click the device type.

Configure device access rule window

In this window, you can configure access rules and schedules for the selected device type.

This window is opened by double-clicking the device type in the **Device type** window.

Device access rules and schedules

Setting	Description
Users and/or user groups	The list contains users and groups for which you can configure access schedule. By default, the table contains the **\Everyone** item (all users). You can add, edit, or delete users or user groups.
Device access rules	This table contains access schedules for users and user groups. It consists of the following columns: • **Access schedule** – names of existing access schedules. The check box next to the schedule indicates whether this schedule is used by the component. • **Access** – access type for the schedule: **Allow** (grant access to devices of the selected type) or **Block** (deny access to devices of the selected type). You can configure schedules only for hard drives, removable drives, floppy disks, and CD/DVD drives. By default, the table contains the **Default** access schedule, which provides all users with full access to devices (the **\Everyone** item is selected in the **Users and/or user groups** list) at any time if access via the connection bus is allowed for this type of device. You can add, edit, or delete access schedules for selected users. The **Default** schedule cannot be modified or removed.

User or group window

In this window, you can specify a user or group of users to which the device access rule applies.

Configure device access rule

Setting	Description
Type	The **User** or **Group** to which the Application Control rule applies.
User or group name	Local user name or user group name to which the rule applies.

Access schedule window

In this window, you can configure the device access schedule.

Schedule for access to devices

Setting	Description
Name	Entry field for the access schedule name.
Time intervals	The table where you can select time intervals for the schedule (days and hours). Intervals highlighted in green are included to the schedule. To exclude an interval from the schedule, click the corresponding cells. Intervals excluded from the schedule are highlighted in gray. By default, all intervals (24/7) are included to the schedule.

Connection buses window

In this window, you can configure access mode for connection buses.

Access mode for connection buses

Setting	Description
Connection bus	Connection bus used by devices to connect to the client device: • **FireWire** • **USB**
Access mode	Connection bus access mode. Right-clicking with the mouse opens a context menu where you can select one of the following items: • **Allow** (default): provide access to devices connected through this bus. • **Block**: deny access to devices connected using this connection bus.

Web Control

In the Administration Console, you can manage Web Control settings in the policy properties (**Security Controls** → **Web Control**).

Web Control component settings

Setting	Description
Enable Web Control	The check box enables the Web Control component. This check box is cleared by default.

Web Control settings	The table contains a list of web resource access rules. Web Control applies rules in the order in which they are listed in the table.
	The table contains the following columns:
	• **Status**. Status of the web resource access rule:
	  • *Enabled* – the rule is enabled, Web Control applies this rule during operation.
	  • *Disabled* – the rule is disabled and is not used when Web Control is running.
	  You can select or clear the check box in the table, you can also select or clear the **Use this rule** check box in the Web Control rule window.
	• **Action**. The action to be taken by the application when it detects an attempt to access web resources that match the rule.
	• **Name**. Web resource access rule name.
	You can add, edit, delete, move up, and move down items in the table.
	You can also import a list of rules from a file by clicking **Advanced** → **Import** and export the list of added rules to a file by clicking **Additional** → **Export selected** or **Additional** → **Export all**. When importing, you will be prompted to replace the list of rules or add the rules to the existing list.

Default rule	In the drop-down list, you can select the default rule that governs how the application regulates access to web resources that are not covered by other rules: • **Allow** (default value) – allow access to the web resources. • **Block** – block access to the web resources.
Message templates	This group of settings contains the **Configure** button. Clicking this button opens the Message templates window.

Web Control rule window

In this window, you can configure the settings of the web resource access rule.

Add Web Control rule

Setting	Description
Rule name	Field for entering the name of the web resource access rule. The rule name must be unique.
Use this rule	This check box enables or disables the use of this rule when the application is running. If the check box is selected, the rule is enabled, and Web Control applies this rule at runtime. If the check box is cleared, the rule is disabled and is not used when Web Control is running. You can enable the use of this Web Control rule later by selecting the check box. This check box is selected by default.
Filter content	In the drop-down list, you can select a content filter for the web resource: • **Do not filter** (default value). If this item is selected, no web resource content filter is used. • **By content category**. When this item is selected, the **Select** button becomes available. Clicking this button opens the Content category selection window. • **By data type category**. When this item is selected, the **Select** button becomes available. Clicking this button opens the Data type category selection window. • **By content category and data type category**. When this item is selected, the **Select** buttons become available. Clicking these buttons opens windows where you can select the necessary categories.
Filter addresses	In the drop-down list, you can select a filter for the address of a web resource: • **Any address** (default value). If this item is selected, the web resource address filter is not used; the Web Control rule is applied to all web resource addresses. • **Specified addresses**. When this item is selected, the **Select addresses** button becomes available. Clicking this button opens the Select addresses window, where you can select the necessary web resource addresses.
Apply to users	In the drop-down list, you can select the users that the web resource access rule applies to: • **All users** (default value). If this item is selected, the user filter is not used; the Web Control rule is applied to all users. • **Selected users**. When this item is selected, the **Select users** button becomes available. Clicking this button opens the Select users window.

Setting	Description
Rule schedule	In the drop-down list, you can configure the schedule for the web resource access rule: • **Always** (default value). When this item is selected, the web resource access rule is applied without time limits, that is, at all times. • **<Schedule name>**. When this item is selected, the **Delete** and **Edit** buttons become available, which you can click to delete or configure the schedule. • **Add new schedule**. Selecting this item opens the Access schedule window where you can configure a new schedule for the web resource access rule.
Rule action	In the drop-down list, you can select the action that Web Control will perform when it detects an attempt to access a web resource that matches the rule: • **Allow** (default value) – allow access to the web resource. • **Block** – block access to the web resource and display a message that access is blocked. • **Inform** – display a warning that the web resource is undesirable. By clicking links in the warning message, the user can access the requested web resource.

Content category selection window

In this window, you can select the content categories for which you want to control access.

To do this, select check boxes next to categories.

All check boxes are cleared by default.

Selecting check boxes for all nested content categories does not automatically select the check box for the parent content category.

Data type category selection window

In this window, you can select the type categories for which you want to control access.

To do this, select check boxes next to categories.

All check boxes are cleared by default.

Select addresses window

In this window, you can specify the addresses of web resources for which you want to control user access. You can specify multiple addresses; enter each address on a new line for convenience of copying them. You can use masks to specify addresses.

If you want to specify a group of addresses, open the **Select address groups** window by clicking the **Add address group** button.

Select address groups window

The table contains groups of addresses of web resources for which user access is controlled by the Web Control component.

If you want to add a group of addresses to the list of groups in the **Select addresses** window, select the check box next to a group name in the table and click the **Add** button below the table.

You can add, edit, or delete items in the table.

If you want to add a new group of addresses to the list of groups in this window, open the **Add address** group window by clicking the **Add** button above the table.

The table is empty by default.

Add address group window

In this window, you can specify the groups of addresses of web resources for which you want to control user access. You can specify multiple addresses in the address group; enter each address on a new line for convenience of copying them. You can use masks to specify addresses.

Select users window

The table contains the names of users and user groups for which access to web resources is controlled according to the rule.

You can add, edit, or delete items in the table

If you want to add a new user and/or user group to the user list in this window, click the **Add** button located above the table to open the **User or group** window.

The table is empty by default.

User or group window

In this window, you can specify a user or group of users to which the web resource access rule applies.

Configuring a web resource access rule

Setting	Description
Type	The **User** or **Group** to which the Application Control rule applies.
User or group name	Name of the user or user group to which the rule applies.

Access schedule window

In this window, you can configure the web resource access schedule.

Web resource access schedule

Setting	Description
Name	Entry field for the access schedule name.
Time intervals	The table where you can select time intervals for the schedule (days and hours). Intervals highlighted in green are included to the schedule. To exclude an interval from the schedule, click the corresponding cells. Intervals excluded from the schedule are highlighted in gray. By default, all intervals (24/7) are included to the schedule.

Application Control

In the Administration Console, you can manage Application Control settings in the policy properties (**Security Controls → Application Control**).

Application Control component settings

Setting	Description
Enable Application Control	The check box enables the Application Control component. This check box is cleared by default.
Action on application startup attempt	The action that Kaspersky Endpoint Security performs upon detecting an attempt to start an application that matches the configured rules: • **Apply rules** (default value). If you select this option, Kaspersky Endpoint Security applies Application Control rules and performs the action specified in the rules. • **Test rules**. If you select this option, Kaspersky Endpoint Security tests the rules and generates an event about an attempt to start an application that matches the rules.
Application Control mode	Application Control task operation mode: • **Allowlist**. If you select this option, Kaspersky Endpoint Security prevents all users from launching any applications except those specified in the Application Control rules. • **Denylist** (default value). If you select this option, Kaspersky Endpoint Security allows all users to launch any applications except those specified in the Application Control rules.
Application Control rules	This group of settings contains the **Configure** button. Clicking this button opens the Application Control rules window.
Applying rules	In the drop-down list, you can select how rules are added: • **Replace local rules with policy rules**. When you select this item, the application applies only the rules specified in the policy. • **Add policy rules to local rules** (default value). If this item is selected, the application applies rules configured in the policy together with local rules configured on the protected device.

Application Control rules window

The **Application Control rules** table contains the rules used by the Application Control component. The Application Control rules table is empty by default.

Application Control rules settings

Setting	Description
Category name	The name of the application category that is used by the rule.
Status	Operation status of the Application Control rule: • *Enabled* – the rule is enabled, Application Control applies this rule during operation. • *Disabled* – the rule is disabled and is not used when the Application Control is running. • *Test* – Application Control allows launching applications that meet the rule criteria, but logs information about launches of these applications in the report. You can change the rule status in the Add new rule window.

You can add, modify, or delete Application Control rules.

Adding rule window

In this window, you can configure the settings for the Application Control rule.

Adding the Application Control rule

Setting	Description
Description	Description of the Application Control rule.
Rule status	In the drop-down list, you can select the status of the Application Control rule: • *Enabled* – the rule is enabled, Application Control applies this rule during operation. • *Disabled* – the rule is disabled and is not used when the Application Control is running. • *Test* – Application Control allows launching applications that meet the rule criteria, but logs information about launches of these applications in the report.
Category	The group of settings contains the **Configure** button. Clicking this button opens the **Application categories** window.
Users and their rights	The table contains a list of users or user groups to which the Application Control rule applies, and the types of access assigned to them, and consists of the following columns: • **User or group name** – names of users or names of user groups to which the Application Control rule applies. • **Access** – the type of access: **Allow** launching the applications or **Block** launching the applications. You can add, edit, or delete users or user groups.

Application categories window

In this window, you can add a new category or configure the category settings for an Application Control rule.

Kaspersky Endpoint Security does not support use of the KL categories of Kaspersky Security Center.

Application Control categories

Setting	Description
Category name	List of the added Application Control categories.
Add	Clicking the button starts the category creation wizard. Follow the instructions of the Wizard. For details about creating a category, refer to the Kaspersky Security Center Help.
Edit	Clicking this button opens the category properties window, where you can change the category settings. The **Golden Image (local)** category cannot be edited.

User or group window

In this window, you can specify a local or domain user or user group for which you want to configure a rule.

Adding the Application Control rule

Setting	Description
Type	The **User** or **Group** to which the Application Control rule applies.
User or group name	Name of the user or user group to which the Application Control rule applies.
Access	Access type: **Allow** launching the applications or **Block** launching the applications.

Inventory

In the Kaspersky Security Center Administration Console, you can perform an inventory of the applications for the protected device using the *Inventory* task.

You can create and run Inventory user tasks. You can manage scan settings by editing the settings of the tasks.

> The Kaspersky Security Center database can store information about up to 150,000 processed files. When this number of records is reached, new files will not be processed. To resume the Inventory task, delete the files registered in the Kaspersky Security Center database as a result of previous inventories, from the device where Kaspersky Endpoint Security is installed.

Inventory task settings

Setting	Description
Action to perform on the "Golden image" category upon task completion	In the drop-down list, you can select the action that Kaspersky Endpoint Security must perform with the Golden Image application category upon completion of the Inventory task: • **No changes** – do not change the Golden Image application category after completing the inventory. This is the default. • **Update or create (if does not exist)** – add applications that the Inventory task discovers on the device to the Golden Image category. If the category does not exist, it is created. If the category exists, the list of applications in the category is updated. • **Delete** – clear the Golden Image category of applications. The category is cleared immediately the task is started, without doing an inventory of files on the device. You can use the Golden Image category in the Application Control rules.
Scan all executables	This check box enables or disables of executable file scans. This check box is selected by default.
Scan binaries	The check box enables or disables scans of binary files (files with the extensions .elf, .java and .pyc). This check box is selected by default.
Scan scripts	This check box enables or disables script scans. This check box is selected by default.
Inventory scopes	The group of settings contains the **Configure** button. Clicking this button opens the **Scan scopes** window.

In the **Exclusions** section for the Inventory task, you can also configure scopes to be excluded from scans.

Scan scopes window

The table contains the scan scopes. The application will scan files and directories located in the paths specified in the table. By default, the table contains one scan scope – /usr/bin.

Scan scope settings for the Inventory task

Setting	Description
Scope name	Scan scope name.
Path	Path to the directory that the application scans.
Status	The status indicates whether the application scans this scope.

You can add, edit, delete, move up, and move down items in the table.

Kaspersky Endpoint Security scans objects in the specified scopes in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

New scan scope window

In this window, you can add and configure scan scope for the Inventory task.

Inventory scope settings

Setting	Description
Scan scope name	Field for entering the scan scope name. This name will be displayed in the table in the Scan scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables the scan of this scope when the task is performed. If this check box is selected, the application processes this scan scope while running the task. If this check box is cleared, the application does not process this scan scope while running the task. You can later include this scope in task settings by selecting the check box. This check box is selected by default.
File system, access protocol, and path	Entry field for the path to the local directory that you want to include in the scan scope. You can use masks to specify the path. The field must not be blank.
Masks	This list contains name masks of the objects that the application scans while running the task. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Exclusions section

Settings of scan exclusions

Group of settings	Description
Exclusion scopes	This group of settings contains the **Configure** button. Clicking this button opens the Exclusion scopes window. In this window, you can define the list of scopes to be excluded from monitoring.

Exclusion scopes window

This window contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table.

Exclusion scope settings

Setting	Description
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from scan.
Status	The status indicates whether the application uses this exclusion.

By default, the table of exclusion scopes is empty. You can add, edit, and delete items in the table.

You can also import the list of exclusions from a file by clicking **Advanced** -> **Import** and export the list of added exclusions to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**.

New exclusion scope window

In this window, you can add and configure scan exclusion scope for the Inventory task.

Exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the Exclusion scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables the exclusion of the scope when the task is executed. If this check box is selected, the application excludes this scope during task execution. If this check box is cleared, the application includes this scope during task execution. You can later exclude this scope from scanning by selecting the check box. This check box is selected by default.
File system, access protocol, and path	Entry field for the path to the local directory that you want to exclude from the inventory. You can use masks to specify the path. The field must not be blank.
Masks	The list contains name masks of the objects that the application excludes from scan. You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

System Integrity Monitoring

In the Administration Console, you can configure System Integrity Monitoring settings in the policy properties (**Security Controls** → **System Integrity Monitoring**).

System Integrity Monitoring settings

Setting	Description
Enable System Integrity Monitoring	This check box enables or disables System Integrity Monitoring. This check box is cleared by default.
Monitoring scopes	The group of settings contains the **Configure** button. Clicking this button opens the Scan scopes window.
Monitoring exclusions	This group of settings contains the **Configure** button. Clicking this button opens the Exclusion scopes window.
Exclusions by mask	This group of settings contains the **Configure** button, which opens the Exclusions by mask window.

Scan scopes window

The table contains monitoring scopes for the System Integrity Monitoring component. The application monitors files and directories located in the paths specified in the table. By default, the table contains one monitoring scope, **Kaspersky internal objects** (/opt/kaspersky/kesl/).

Monitoring scope settings

Setting	Description
Merge inherited values	This check box enables or disables the merging of the list when inherited in child policies. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.
Scope name	Monitoring scope name.
Path	Path to the directory that the application protects.
Status	The status indicates whether the application scans this scope.

You can add, edit, delete, move up, and move down items in the table.

Kaspersky Endpoint Security scans objects in the specified scopes, in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

New scan scope window

In this window, you can add and configure monitoring scopes for the System Integrity Monitoring component.

Monitoring scope settings

Setting	Description
Scan scope name	Field for entering the monitoring scope name. This name will be displayed in the table in the **Scan scopes** window. The entry field must not be blank.
Use this scope	This check box enables or disables scans of this scope by the application. If this check box is selected, the application controls this monitoring scope during the application's operation. If this check box is cleared, the application does not control this monitoring scope during the operation. You can later include this scope in the component settings by selecting the check box. This check box is selected by default.
File system, access protocol, and path	Entry field for the path to the local directory that you want to include in the monitoring scope. The field must not be blank. The default path is /opt/kaspersky/kesl.
Masks	The list contains name masks for the objects that the application scans. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Exclusion scopes window

The window contains monitoring exclusion scopes for the System Integrity Monitoring component. The application does not scan files and directories located at the paths specified in the table.

Monitoring exclusion scope settings

Setting	Description
Merge inherited values	This check box enables or disables the merging of the list when inherited in child policies. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from monitoring.
Status	Indicates whether the application excludes this scope from monitoring during the component operation.

By default, the table of exclusion scopes is empty. You can add, edit, or delete items in the table.

You can also import the list of exclusion scopes from a file by clicking **Import** or export the list of exclusion scopes to a file in JSON format by clicking **Export**. When importing, you are prompted to replace the list of exclusion scopes or add exclusion scopes to the existing list.

New exclusion scope window

In this window, you can add or configure the monitoring exclusion scope for the System Integrity Monitoring component.

Monitoring exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the **Exclusion scopes** window. The entry field must not be blank.
Use this scope	The check box enables or disables the exclusion of the scope from monitoring when the application is running. If this check box is selected, the application excludes this scope from monitoring during the component operation. If this check box is cleared, the application monitors this scope during the component operation. You can later exclude this scope from monitoring by selecting the check box. This check box is selected by default.
File system, access protocol, and path	Entry field for the path to the local directory that you want to add to the exclusion scope. The field must not be blank. The **/** path is specified by default. The application excludes all directories of the local file system from scan.
Masks	The list contains name masks of the objects that the application excludes from the monitoring. By default the list contains the * mask (all objects). You can add, edit, or delete masks. Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from monitoring. Examples: The `*.txt` mask refers to all text files. The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

Exclusions by mask window

You can configure the exclusion of objects from monitoring based on name masks. The application does not scan the files with the names containing the specified masks. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from monitoring.

Examples:
The `*.txt` mask refers to all text files.
The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

You can also import the exclusion list from a file using the **Import** button and export the exclusion list to a JSON file using the **Export** button. When importing, you will be prompted to replace the list of exclusions or add the exclusions to the existing list.

You can enable the merging of the list of exclusions when inherited by child policies. If you want to merge list items, select the **Merge inherited values** check box. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.

System Integrity Check

You can perform a system integrity check in the Administration Console, with the help of the *System Integrity Check* task.

You can create and run custom System Integrity Check tasks. You can manage scan settings by editing the settings of the tasks.

In the **Settings** section of the properties of the System Integrity Check task, you can edit the settings listed in the table below.

System Integrity Check task settings

Setting	Description
Rebuild baseline on each task start	This check box enables or disables the rebuilding of the system baseline every time the System Integrity Check task is started. This check box is cleared by default.
Check SHA256 hash	This check box enables or disables the use of the file hash as a criterion when comparing the current state of the file with its original state. If this check box is cleared, the application compares only the file size (if the file size has not changed, then the modification time is not considered a critical parameter). This check box is cleared by default.
Track directories in monitoring scopes	This check box enables or disables scanning of directories within the specified monitoring scopes during a system integrity check. This check box is cleared by default.
Track the last time a file was accessed	This check box enables or disables tracking the file access time while the system integrity check runs. This check box is cleared by default.
Monitoring scopes	The group of settings contains the **Configure** button. Clicking this button opens the Scan scopes window.

In the Exclusion scopes sections in the properties of the System Integrity Check, you can define monitoring exclusions and exclusions by mask.

Scan scopes window

The table contains monitoring scopes for the System Integrity Check task. The application monitors files and directories located in the paths specified in the table. By default, the table contains one monitoring scope, **Kaspersky internal objects** (/opt/kaspersky/kesl/).

Monitoring scope settings

Setting	Description
Scope name	Monitoring scope name.
Path	Path to the directory that the application protects.
Status	The status indicates whether the application scans this scope.

You can add, edit, delete, move up, and move down items in the table.

Kaspersky Endpoint Security scans objects in the specified scopes, in the order they appear in the list of scopes. If necessary, place the subdirectory higher in the list than its parent directory, to configure security settings for a subdirectory that are different from the security settings of the parent directory.

New scan scope window

In this window, you can add and configure monitoring scopes for the System Integrity Check task.

Monitoring scope settings

Setting	Description
Scan scope name	Field for entering the monitoring scope name. This name will be displayed in the table in the Scan scopes window. The entry field must not be blank.
Use this scope	This check box enables or disables scans of this scope by the application. If this check box is selected, the application controls this monitoring scope during the application's operation. If this check box is cleared, the application does not control this monitoring scope during the operation. You can later include this scope in the component settings by selecting the check box. This check box is selected by default.
File system, access protocol, and path	Entry field for the path to the local directory that you want to include in the monitoring scope. You can use masks to specify the path. The field must not be blank. The default path is /opt/kaspersky/kesl.
Masks	The list contains name masks for the objects that the application scans. By default the list contains the * mask (all objects). You can add, edit, or delete masks.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Exclusions section

Settings of scan exclusions

Group of settings	Description
Monitoring exclusions	This group of settings contains the **Configure** button. Clicking this button opens the Exclusion scopes window. In this window, you can define the list of scopes to be excluded from monitoring.
Exclusions by mask	This group of settings contains the **Configure** button, which opens the Exclusions by mask window. In this window, you can configure the exclusion of objects from monitoring by name mask.

Exclusion scopes window

The table contains scan exclusion scopes for the System Integrity Check component. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

Scan exclusion scope settings for the System Integrity Check task

Setting	Description
Exclusion scope name	Exclusion scope name.
Path	Path to the directory excluded from scan.
Status	Indicates whether the application excludes this scope from monitoring during the component operation.

You can add, edit, or delete items in the table.

New exclusion scope window

In this window, you can add and configure the monitoring exclusion scope for the System Integrity Check task.

Monitoring exclusion scope settings

Setting	Description
Exclusion scope name	Field for entering the exclusion scope name. This name will be displayed in the table in the Exclusion scopes window. The entry field must not be blank.
Use this scope	The check box enables or disables the exclusion of the scope from monitoring when the application is running. If this check box is selected, the application excludes this scope from monitoring during the task operation. If this check box is cleared, the application monitors this scope during the task operation. You can later exclude this scope from monitoring by selecting the check box. This check box is selected by default.
File system, access protocol, and path	Entry field for the path to the local directory that you want to add to the exclusion scope. You can use masks to specify the path. The field must not be blank. The **/** path is specified by default. The application excludes all directories of the local file system from scan.
Masks	The list contains name masks of the objects that the application excludes from the monitoring. By default the list contains the ***** mask (all objects). You can add, edit, or delete masks. Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans. Examples: The `*.txt` mask refers to all text files. The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Exclusions by mask window

You can configure the exclusion of objects from monitoring based on name masks. The application does not scan the files with the names containing the specified masks. By default, the list of masks is empty.

You can add, edit, or delete masks.

Clicking the **Add** button opens the **Object mask** window. In this window, in the **Define object mask** field, you can specify the name template for files that Kaspersky Endpoint Security excludes from scans.

Examples:
The `*.txt` mask refers to all text files.
The `*_my_file_??.html` mask refers to html files starting with any characters, and ending with `_my_file_` followed by any two characters (for example, 2020_my_file_09.html).

Local Tasks

Task management

In the Administration Console, you can set the permission to view and manage tasks in the policy properties (**Local Tasks** → **Task management**).

Task management settings

Setting	Description
Allow local tasks	This check box allows or blocks the users from viewing local tasks created in Kaspersky Endpoint Security and control of these tasks on the managed client devices. If this check box is selected, users can configure and run tasks in the graphical interface of the application and on the command line. If this check box is cleared, local tasks are not used. Scheduled local tasks do not run. Tasks cannot be run or configured in the graphical interface of the application or on the command line. This check box is cleared by default.
Allow viewing and managing tasks created through KSC	This check box allows or prohibits the users from viewing the tasks created in Kaspersky Security Center and managing these tasks on client devices. If this check box is selected, tasks created in Kaspersky Security Center are displayed in the graphical interface of the application. Users can start and stop these tasks from the graphical interface of the application and from the command line. If this check box is cleared, tasks created in Kaspersky Security Center cannot be viewed or managed in the graphical interface of the application or on the command line. This check box is cleared by default.

Protection against advanced threats and targeted attacks

Integration with Kaspersky Managed Detection and Response

In the Administration Console, you can enable or disable the MDR component and upload the MDR BLOB file in the policy properties (**Detection and Response** → **Managed Detection and Response**).

MDR integration settings

Setting	Description
Enable Managed Detection and Response	This check box enables or disables the MDR component, which is necessary for integrating Kaspersky Endpoint Security with the Kaspersky Managed Detection and Response solution. The component is disabled by default. If you enable the MDR component and Kaspersky Security Network is disabled or used in standard mode, you are prompted to accept the Kaspersky Security Network Statement to enable Kaspersky Security Network in Extended mode. If changing KSN settings is prohibited by parent policy, an error message is displayed and the MDR component is not enabled.
Upload	Clicking this button opens a standard Microsoft Windows window in which you can select an MDR BLOB file to upload. This action is mandatory if you have tenants or if you have activated the MDR component using the MDR BLOB file.

The BLOB file can be found inside the ZIP archive of the MDR configuration file included in the Kaspersky Managed Detection and Response distribution kit.

By uploading the BLOB file, you agree that data from the device where Kaspersky Endpoint Security is installed will be automatically sent to Kaspersky for processing. Do not upload the file if you do not agree to the processing of transmitted data. For detailed description of the transmitted data, refer to Kaspersky Managed Detection and Response help section.

Kaspersky Endpoint Detection and Response (on-premises) Integration

In the Administration Console, you can enable or disable the EDR Expert (on-premises) component and manage the settings for integrating the Kaspersky Endpoint Security application with the Kaspersky Endpoint Detection and Response (KATA) component in the policy properties (**Detection and Response** → **EDR Expert (on-premises)**).

If **Endpoint Detection and Response Expert (version 8.0 and higher)** is selected in the Web Console for the EDR Expert (on-premises) component, that is, the EDR Expert (on-premises) integration mode is selected, the Administration Console displays a warning, and the settings for the Kaspersky Endpoint Detection and Response (KATA) integration are not available. You can change the integration mode in the Web Console.

Kaspersky Endpoint Detection and Response (on-premises) Integration settings

Setting	Description
Enable Endpoint Detection and Response Expert (on-premises)	This check box enables or disables the EDR Expert (on-premises) component that provides integration with Kaspersky Endpoint Detection and Response (KATA). The component is disabled by default.
Enable Execution Prevention for objects	This check box enables or disables EDR Expert (on-premises) rules for execution prevention for objects.
KATA servers	The **Configure** button opens a window where you can configure a connection to KATA servers, as well as view a list of servers to which a connection has been configured.
Server connection settings	Clicking the **Configure** button opens a window where you can configure general settings for connecting to KATA servers, add a server certificate, and configure two-way authentication when connecting to KATA servers.
Data transfer settings	Clicking the **Configure** button opens a window where you can configure settings for transfer of data to KATA servers.

Configuring the KATA server connection

The table lists connection settings for KATA servers. For each server for which a connection is configured, the table indicates an IP address (IPv4 or IPv6) or the server's fully qualified domain name (FQDN) and port.

You can use the buttons and the menu above the table to perform the following actions:

- Add KATA server connection settings
- Edit or remove previously configured connection settings
- Export or import the list of configured connection settings

Server connection settings

Setting	Description
Address	KATA server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. To ensure that communication with the server is not interrupted in the event of an application failure while network isolation is enabled on the device, we recommend specifying the server's IP address. Default value: `127.0.0.1`.
Port	Port to connect to the KATA server. Default value: `443`.

Managing general KATA server connection settings

In this window, you can configure general settings for connecting to KATA servers.

KATA server connection settings

Setting	Description
Send a synchronization request to the KATA server every (min)	Frequency of sending synchronization requests to the KATA server in minutes. Default value: `5`.
Maximum time to wait for the server connection (sec)	Maximum time to wait for a connection to the KATA server in seconds. Default value: `10`.
Maximum time to wait for a response from the server (sec)	Maximum time to wait for a response from the KATA server in seconds. Default value: `10`.

Setting	Description
Allow sending telemetry	This check box enables or disables sending data about events on devices (telemetry) to the KATA server. Sending telemetry is enabled by default.

Server certificate	The section contains buttons for adding or removing a server certificate:
	• **Add** opens the window in which you can add a server certificate. The button is displayed if the server certificate has not been added yet.
	In the window for adding a certificate, you can add a KATA server certificate in one of the following ways:
	  • In the **Add from file** field, specify the path to the certificate file containing the certificate in DER or PEM format. The **Browse** button opens the standard file selection window.
	  • Copy the contents of the certificate file into the **Enter certificate details** field.
	If a server certificate has been added, the server certificate is verified on the Kaspersky Endpoint Security side. This elevates the security of the connection.
	• **Delete** deletes the server certificate added previously. The button is displayed only if a server certificate has been added.

Additional connection protection	This section contains controls for configuring additional security of the connection using two-way authentication:
	• **Use two-way authentication** enables or disables two-way authentication to further secure the connection to the KATA server. To use two-way authentication, you need to add a client certificate.
	  Two-way authentication must be enabled on the KATA server side.
	• **Add** opens the window for adding a client certificate for additional security of the connection with the KATA server. The button is displayed if the **Use two-way authentication** check box is selected and the client certificate has not yet been added.
	To add a client certificate, in the window for adding a certificate, specify the path to the cryptocontainer (PFX archive) containing the client certificate and private key. The **Browse** button opens the standard file selection window. Next, enter the client certificate password in the **Crypto container password** field.
	  The field is mandatory. An error message is displayed if you try to save the settings without entering a password.
	If the password is correct, the **OK** button becomes active. You can save the settings.
	• **Delete** deletes the previously added client certificate. This button is displayed only if a client certificate has been added.

Configuring data transmission to KATA servers

In this window, you can configure settings for sending data to KATA servers.

Settings for sending data to KATA servers

Setting	Description
Maximum delay when sending events (sec)	The maximum delay in sending events to the KATA server in seconds. Default value: `30`.
Enable event throttling	Enables or disables the regulation of the number of events sent to the KATA server.
Maximum number of events per hour	Maximum number of events per hour Default value: `3000`.
Number of events above the limit (percentage)	Number of events above the limit (percentage). Sending events is limited if ratio of events of one type (for example, events about registry changes) to the total number of events exceeds the set threshold (as a percentage). Default value: `15`.

Kaspersky Network Detection and Response (KATA) Integration

In the Administration Console, you can enable or disable the NDR (KATA) component and manage the settings for integrating the Kaspersky Endpoint Security application with the Kaspersky Network Detection and Response (KATA) component in the policy properties (**Detection and Response** → **Network Detection and Response (KATA)**).

Kaspersky Network Detection and Response (KATA) integration settings

Setting	Description
Enable Network Detection and Response (KATA)	This check box enables or disables the NDR (KATA) component. The component is disabled by default.
NDR servers	The **Configure** button opens a window where you can configure a connection to NDR servers, as well as view a list of servers to which a connection has been configured.
Server connection settings	Clicking the **Configure** button opens a window where you can configure general settings for connecting to NDR servers, add a server certificate, and configure two-way authentication when connecting to NDR servers.
Data transfer settings	Clicking the **Configure** button opens a window where you can configure settings for transfer of data to NDR servers.

Configuring the NDR server connection

The table lists connection settings for NDR servers. For each server for which a connection is configured, the table indicates an IP address (IPv4 or IPv6) or the server's fully qualified domain name (FQDN) and port.

You can use the buttons and the menu above the table to perform the following actions:

- Add NDR server connection settings
- Edit or remove previously configured connection settings
- Export or import the list of configured connection settings

Server connection settings

Setting	Description
Address	NDR server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. Default value: `127.0.0.1`.
Port	Port to connect to the NDR server. Default value: `443`.

Managing general NDR server connection settings

In this window, you can configure general settings for connecting to NDR servers.

NDR server connection settings

Setting	Description
Send a synchronization request to the NDR server every (min)	Frequency of sending synchronization requests to the NDR server in minutes. Default value: `5`.
Maximum time to wait for the server connection (sec)	Maximum time to wait for a connection to the NDR server in seconds. Default value: `10`.
Maximum time to wait for a response from the server (sec)	Maximum time to wait for a response from the NDR server in seconds. Default value: `10`.

Server certificate	The section contains buttons for adding or removing a server certificate:
	• **Add** opens the window in which you can add a server certificate. The button is displayed if the server certificate has not been added yet.
	In the window for adding a certificate, you can add an NDR server certificate in one of the following ways:
	  • In the **Add from file** field, specify the path to the certificate file containing the certificate in DER or PEM format. The **Browse** button opens the standard file selection window.
	  • Copy the contents of the certificate file into the **Enter certificate details** field.
	If a server certificate has been added, the server certificate is verified on the Kaspersky Endpoint Security side. This elevates the security of the connection.
	• **Delete** deletes the server certificate added previously. The button is displayed only if a server certificate has been added.

Additional connection protection	This section contains controls for configuring additional security of the connection using two-way authentication: • **Use two-way authentication** enables or disables two-way authentication to further secure the connection to the NDR server. To use two-way authentication, you need to add a client certificate. Two-way authentication must be enabled on the NDR server side. • **Add** opens the window for adding a client certificate for additional security of the connection with the NDR server. The button is displayed if the **Use two-way authentication** check box is selected and the client certificate has not yet been added. To add a client certificate, in the window for adding a certificate, specify the path to the cryptocontainer (PFX archive) containing the client certificate and private key. The **Browse** button opens the standard file selection window. Next, enter the client certificate password in the **Crypto container password** field. The field is mandatory. An error message is displayed if you try to save the settings without entering a password. If the password is correct, the **OK** button becomes active. You can save the settings. • **Delete** deletes the previously added client certificate. This button is displayed only if a client certificate has been added.

Configuring data transmission to NDR servers

In this window, you can configure settings for sending data to NDR servers.

Settings for sending data to NDR servers

Setting	Description
Maximum delay when sending events (sec)	The maximum delay in sending events to the NDR server in seconds. Default value: `30`.
Maximum number of events in package	Maximum number of events in one package. Default value: `1024`.
Server poll frequency	Frequency of sending synchronization requests to the NDR server in seconds. Default value: `450`.
Enable event throttling	Enables or disables the regulation of the number of events sent to the NDR server.

Setting	Description
Maximum number of events per hour	Maximum number of events per hour Default value: `3000`.
Number of events above the limit (percentage)	Number of events above the limit (percentage). Sending events is limited if ratio of events of one type (for example, events about registry changes) to the total number of events exceeds the set threshold (as a percentage). Default value: `15`.

Integration with KUMA

In the Administration Console, you can enable or disable the integration of Kaspersky Endpoint Security with Kaspersky Unified Monitoring and Analysis Platform and manage integration settings in the policy properties (**KUMA Integration** → **KUMA Integration**).

Settings for integration with Kaspersky Unified Monitoring and Analysis Platform

Setting	Description
Enable KUMA Integration	Enables or disables the integration of the Kaspersky Endpoint Security application with the Kaspersky Unified Monitoring and Analysis Platform solution. KUMA Integration is disabled by default.
Use encrypted connection	The check box enables or disables server certificate verification for additional protection of the connection to the KUMA server. To verify the server certificate, you need to select this check box and add the server certificate in the **KUMA servers** window. This check box is cleared by default.
KUMA servers	The **Configure** button opens the **KUMA servers** window. In this window, you can configure a connection to KUMA servers and view the list of servers to which a connection is configured.
KUMA server connection settings	Clicking the **Configure** button opens the **Server connection settings** window where you can configure general settings for connecting to KUMA servers, add a server certificate, and configure two-way authentication when connecting to KUMA servers.
Maximum delay when sending events (sec)	The maximum delay in sending events to the KUMA server in seconds. Default value: `30`.

KUMA servers window

The table in the window displays the list of settings for connecting to KUMA servers. For each server to which a connection is configured, the table indicates:

- IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the server. If you selected the Use encrypted connection check box in the **KUMA integration settings** window, you must specify the fully qualified domain name (FQDN) of the server from the certificate received when purchasing the license to use KUMA.
- Port to connect to the KUMA server.
- Protocol used to connect to the KUMA server.

You can use the buttons and the menu above the table to perform the following actions:

- Add KUMA server connection settings
- Edit or remove previously configured connection settings
- Export or import the list of configured connection settings

KUMA server window

In this window you can specify the KUMA server connection settings.

KUMA server connection settings

Setting	Description
Address	KUMA server address IP address (IPv4 or IPv6) or fully qualified domain name (FQDN) of the integration server can be specified. If you selected the Use encrypted connection check box in the **KUMA integration settings** window, you must specify the fully qualified domain name (FQDN) of the server from the certificate received when purchasing the license to use KUMA.
Port	Port to connect to the KUMA server. Default value: `443`.
Protocol	Protocol for connecting to the KUMA server: TCP, UDP, or HTTP/HTTPS with compression. When selecting the UDP protocol, the use of certificates to provide connection protection is not supported, and there are no events about the connection to the KUMA server. The default is TCP.

KUMA server connection settings window

In this window, you can configure general settings for connecting to KUMA servers.

KUMA server connection settings

Setting	Description
Maximum time to wait for the server connection (sec)	Maximum time to wait for a connection to the KUMA server in seconds. Default value: `5`.
Server certificate	The section contains buttons for adding or removing a server certificate.
Add (server certificate)	Opens adding a server certificate window. The button is displayed if the server certificate has not been added yet.
Remove (server certificate)	Removes the server certificate. The button is displayed only if a server certificate has been added.
Additional connection protection	This section contains controls for configuring additional security of the connection using two-way authentication.
Use two-way authentication	The check box enables or disables the use of two-way authentication for additional protection of the connection to the KUMA server. To use two-way authentication, you need to add a client certificate. Two-way authentication must be enabled on the KUMA server side.

Setting	Description
Add (client certificate)	Opens the window for adding a client certificate for security of the connection with the KUMA server. The button is displayed if the client certificate has not been added yet. If you want to configure additional protection for the connection, enable verification of the client certificates on the KUMA server side and select the **Use two-way authentication** check box in this window.
Remove (client certificate)	Removes the client certificate. The button is displayed if a client certificate has been added.

Adding a server certificate window

In this window, you can add a KUMA server certificate in one of the following ways:

- Specify the path to the certificate file in the **Add from file** field. The **Browse** button opens the standard file selection window. Specify the path to the file that contains the certificate in DER or PEM format.
- Copy the contents of the certificate file to the **Enter certificate details** field.

If a server certificate has been added, the server certificate is verified on the Kaspersky Endpoint Security side. This elevates the security of the connection.

Adding a client certificate window

In this window, you can add a client certificate to further secure the connection with the KUMA server.

If you want to configure additional protection for the connection, enable verification of the client certificates on the KUMA server side and select the **Use two-way authentication** check box in the KUMA server connection settings window.

To add a client certificate, specify the path to the cryptocontainer (PFX archive) containing the client certificate and private key. The **Browse** button opens the standard file selection window. Next, enter the client certificate password in the **Crypto container password** field.

The field is mandatory. An error message is displayed if you try to save the settings without entering a password.

If the password is correct, the **OK** button becomes active. You can save the settings.

Quarantine

In the Administration Console, you can manage Quarantine settings in the policy properties (**General settings** → **Storage settings**) and in managed device properties (**Managed devices** → **Devices** tab → device properties window → **Applications** section → application properties window → **Storage settings**).

Quarantine settings

Setting	Description
Limit the size of Quarantine to (MB):	This check box enables or disables limiting the maximum size of the Quarantine to the specified value (in megabytes). If the check box is cleared, the size of quarantine is not limited. Possible values: 1–999999. The default value is 200 if the application is being used in Standard mode or in EDR Agent mode, and 100 if the application is being used in Light Agent mode.
Notify when quarantine is (%) full:	This check box enables or disables the limit on the percentage of Quarantine that must be full to generate an event about Quarantine being full. If the check box is cleared, the event about Quarantine being full is not generated. Possible values: 1–100. Default value: 90.

Execution prevention for objects

You can enable or disable execution prevention for objects in the Administration Console only if integration with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA) is enabled.

You can enable or disable object execution prevention in the policy properties (**Application settings** → **Detection and Response** → **EDR Expert (on-premises)**).

The **Enable Execution Prevention for objects** check box under **Execution Prevention for objects** enables or disables EDR Expert (on-premises) rules for execution prevention for objects.

General settings

In the Administration Console, you can manage general application settings that define the operation of the application as a whole and the operation of individual functions, in the in the policy properties (**General settings**).

Proxy server

In the Administration Console, you can manage proxy server settings in the policy properties (**General settings** → **Proxy server settings**).

Proxy server settings

Setting	Description
Do not use proxy server	If this option is selected, the application does not use a proxy server.
Use the specified proxy server settings	If you select this option the application uses the specified proxy server settings to connect to Kaspersky activation servers, to update sources for databases and application modules, to Kaspersky Security Network, and when verifying website certificates using the Web Threat Protection component.
Address and port	Fields for entering the proxy server's IP address or domain name as well as its port. Default port: 3128. These fields are available if the **Use the specified proxy server settings** option is selected.

Setting	Description
Use proxy server authentication	This check box enables or disables proxy server authentication using a user name and password. This check box is available if the **Use the specified proxy server settings** option is selected. This check box is cleared by default. When connecting via an HTTP proxy, we recommend to use a separate account that is not used to sign in to other systems. An HTTP proxy uses an insecure connection, and the account may be compromised.
User name	Entry field for the user name used for proxy server authentication. The entry field is available if the **Use proxy server authentication** check box is selected.
Password	Entry field for entering the user password for proxy server authentication. It is recommended to make sure that the password complexity and anti-bruteforce mechanisms ensure that the password cannot be guessed within 6 months. Clicking the **Show** button causes the user's password to be displayed in clear text in the **Password** field. By default, the user password is hidden and is displayed as asterisks. The text box and the button are available if the **Use proxy server authentication** check box is selected.
Use Kaspersky Security Center as a proxy server for application activation	Enables or disables the use of Kaspersky Security Center Administration Server as a proxy server for accessing Kaspersky activation servers. This is necessary when activating the application in an isolated network segment without internet access using an activation code. If this check box is selected, the application gains access to activation servers via the Administration Server that has internet access. This check box is cleared by default. This setting applies only if the application is used in standard mode. If the application is used in Light Agent mode, the license information is provided by the Protection Server.
Proxy server exclusions	This group of settings contains the **Configure** button, which opens the Proxy server exclusions window.

Proxy server exclusions window

In this window, you can configure the use of a proxy server when integrated with components of the Kaspersky Anti Targeted Attack Platform solution, as well as a list of addresses for which you want to bypass the proxy server.

Proxy server exclusions

Setting	Description
Do not use proxy server for components	Select the check boxes next to those application components that you do not want to use the proxy server: • **Endpoint Detection and Response Expert (on-premises)** – do not use a proxy server when connecting to servers that provide integration with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA). • **Sandbox** – do not use a proxy server when connecting to servers that provide interaction with Sandbox. • **Network Detection and Response (KATA)** – do not use a proxy server when connecting to Kaspersky Network Detection and Response (KATA) integration servers.
Do not use proxy server for addresses	This table contains a list of addresses to be connected to bypassing the proxy server. • **IP address/DNS name** is the IP address or DNS name to which you want to connect without a proxy server. You can use masks (`*` and `?` characters) to specify addresses. • You can optionally enter a comment in the **Comment** field. You can add, edit, or delete addresses in the table.

CPU usage by scan tasks

In the Administration Console, you can enable or disable the CPU utilization limit and configure the memory usage limit for scan tasks in the policy properties (**General settings** → **Application settings**, **Performance** section).

Clicking **Configure** under **Performance** opens the **Performance settings for scan tasks** window, in which you can configure limits in the **CPU and memory usage** section (see table below).

CPU and memory usage settings

Setting	Description
Limit CPU usage by scan tasks (%)	This check box enables or disables the CPU utilization limit for the *Malware Scan*, *Critical Areas Scan*, *Inventory*, and *Container Scan* tasks. If the check box is selected, the maximum utilization of all processor cores will not exceed the percentage specified in the field on the right. The value in the field must be an integer from 10 to 100. This check box is cleared by default.
Memory usage limit for scan tasks (MB)	Input field for the memory usage limit for scan tasks (in megabytes). Default value: 8192.

Running tasks on battery power

In the Administration Console, you can configure the cancellation of scheduled tasks in the policy properties (**General settings** → **Application settings**, **Performance** section).

Task settings when running on battery power

Setting	Description
Skip scheduled tasks while running on battery power	This check box enables or disables the cancellation of scheduled tasks. This check box is selected by default. If this check box is cleared, all tasks run as scheduled, regardless of whether the device is running on battery power.

Starting the application

In the Administration Console, you can manage application startup settings in the policy properties (**General settings** → **Application settings**, **Application startup settings** section).

Under **Application startup settings**, clicking the **Configure** button opens the **Application startup settings** window, in which you can edit the application startup settings (see the table below).

Application startup settings

Setting	Description
Maximum consecutive unsuccessful attempts to start the application	The input field for the maximum number of consecutive unsuccessful attempts to start the application. Default value: 5.
Maximum time to wait for application start (min)	The input field for the maximum time to wait for the application to start (in minutes), after which the kesl process will be restarted. Default value: 3.

Automatically restarting when a critical update is received

In the Administration Console, you can configure automatic restart of the application when installing critical updates in the policy properties (**General settings** → **Application settings**).

In the **Advanced application settings** section, clicking the **Configure** button opens the **Additional settings** window, in which you can configure the application to restart when critical updates are received (see the table below).

Settings for applying critical updates

Setting	Description
Automatically restart the application when receiving critical updates	The check box enables or disables the automatic application restart when critical updates are received after the first 24 hours after installing the application. This check box is cleared by default. If this check box is selected, the application restarts after critical updates if 24 hours have passed after installation.

Password protection

In the Administration Console, you can configure the Password protection settings in the policy properties (**General settings** → **Interface**, **Password protection** section).

Under **Password protection**, clicking the **Configure** button opens the **Password protection settings** window, in which you can edit the Password protection settings (see the table below).

Application startup settings

Setting	Description
Enable password protection	This check box enables or disables password protection of application settings. This check box is cleared by default.
Permissions	This table contains users and groups for which you can configure permissions to change application settings. The table includes the following columns: • **User / Group** is the name of the local or domain user or the name of the group of users for which permissions are configured. • **Type** is either **User** or **Group** for which permissions are configured. • **Permissions** is a list of operations that the user or group is allowed perform. You can add, edit, and delete users or user groups. You can click the **Add** button to open the **Permissions of a user / group** window in which you can add a user or a group and set permissions to change application settings.

Trace and dump settings

In the Administration Console, you can manage trace and dump settings in the policy properties (**General settings** → **Application settings**, the **Trace and dump settings** section).

Under **Trace and dump settings**, clicking **Configure** opens the **Trace and dump settings** window in which you can edit the trace dump settings (see the table below).

Trace and dump settings

Setting	Description
Path to the trace file directory	Input field for the path to the directory where the trace files are stored. Default value: /var/log/kaspersky/kesl. If you specify a different directory, make sure that the user running Kaspersky Endpoint Security has read and write permissions for that directory. Root privileges are required to access the default trace files directory.
Maximum trace file size (MB)	In this field, you can enter the maximum size of an application trace file (in megabytes). Default value: 500.
Maximum number of trace files	In this field, you can enter the maximum number of application trace files. Default value: 10.
Create a dump file if the application crashes	This check box enables or disables the creation of a dump file when the application crashes. This check box is cleared by default.
Path to the dump file directory	Input field for the path to the directory where the dump files are stored. The input field is limited to 128 characters. Default value: /var/opt/kaspersky/kesl/common/dumps.

Resident memory usage by the application

In the Administration Console, you can configure the resident memory usage limit in the policy properties (**General settings** → **Application settings**).

In the **Advanced application settings** section, clicking the **Configure** button opens the **Additional settings** window, in which you can configure the resident memory usage limit (see the table below).

To apply the changes, restart the Kaspersky Endpoint Security application on the managed device after the policy has been applied.

Settings for resident memory usage by the application

Setting	Description
Application memory usage	In the drop-down list, you can select how to limit resident memory usage: • **Unlimited**. If this option is selected, resident memory usage is not limited. • **Limited automatically (recommended)**. When this item is selected, resident memory usage is limited automatically (default value). • **Limited to a percentage of total**. When this item is selected, the **Memory usage limit (%)** field becomes available, in which you can specify the necessary value as a percentage. • **Limited to a value in MB**. When this item is selected, the **Memory usage limit (MB)** field becomes available, in which you can specify the desired value in megabytes. • **Limited to whichever is lowest (%, MB)**. When this item is selected, the **Memory usage limit (%)** and **Memory usage limit (MB)** fields become available, in which you can specify the necessary values. • **Limited to whichever is highest (%, MB)**. When this item is selected, the **Memory usage limit (%)** and **Memory usage limit (MB)** fields become available, in which you can specify the necessary values.
Memory usage limit (%)	Input field for the memory usage limit (as a percentage). Default value: 50.
Memory usage limit (MB)	Input field for the memory usage limit (in megabytes). Default value: 2000.

Encrypted connections scan

In the Administration Console, you can manage network traffic scan settings in the policy properties (**General settings** → **Network settings**).

Encrypted connections scan settings

Setting	Description
Enable encrypted connection scans	This check box enables or disables encrypted connection scans. This check box is selected by default.

Settings for encrypted connections	This section contains the encrypted connections scan settings:
	• **Visit to a domain with an untrusted certificate** specifies the action that the application must perform when a domain with an untrusted certificate is visited:
	  • **Allow** (default value) — Allow connecting to the domain with an untrusted certificate.
	  • **Block** — Block connection to the domain with an untrusted certificate.
	• **Visit to a domain with a network traffic scan error** specifies the action that the application must perform when a domain with a network traffic scan error is visited:
	  • **Allow and add domain to exclusions** (default value) — Add the domain that resulted in the error to the list of domains with scan errors and do not scan encrypted network traffic when this domain is visited.
	  • **Block** — Block connection to the domain with a scan error.
	• **Certificate verification policy** is the method the application uses to verify certificates:
	  • **Local check**: the application does not use the internet to verify a certificate.
	  • **Full check** (default value): the application uses the internet to check and download the missing chains that are needed to verify a certificate.

Trusted domains	This group of settings contains the **Configure** button, which opens the Trusted domains window, where you can configure the list of trusted domain names.
Trusted root certificates	This group of settings contains the **Configure** button. Clicking this button opens the Trusted root certificates window. In this window, you can configure the list of root certificates that Kaspersky Endpoint Security must consider trusted when scanning encrypted connections.
Traffic interception exclusions	This group of settings contains the **Configure** button, which you can click to open the Traffic interception exclusions window. In this window, you can manage the settings of connections that the application excludes from traffic interception.
Network ports settings	This group of settings contains the **Configure** button. Clicking this button opens the Monitored ports window.
Advanced settings	This group of settings contains the **Configure** button, which you can click to open the **Traffic interception mode** window. In this window, you can configure the traffic interception mode: • **Use eBPF**. If this option is selected, the application uses the eBPF technology to intercept traffic. • **Use iptables** (default). If this option is selected, the application uses the iptables technology to intercept traffic. To change the traffic interception mode, you need to restart the application. Restarting breaks established network connections.

Trusted domains window

This list contains the domain names and domain name masks that will be excluded from scanning. The application does not scan connections established when visiting specified domains.

Example: `*example.com`. For example, `*example.com/*` is incorrect because a domain address, not a web page, needs to be specified.

By default, the list is empty. You can add, edit, or remove domains from the list of trusted domains.

Trusted certificates window

You can configure a list of root certificates considered trusted by Kaspersky Endpoint Security. The list of trusted root certificates is used when scanning encrypted connections.

The following information is displayed for each certificate:

- Certificate subject
- Certificate serial number
- Certificate issuer
- Certificate start date
- Certificate expiration date
- SHA256 certificate fingerprint

By default, the certificate list is empty.

You can add or remove certificates.

Clicking the **Add** button opens a window in which you can add a certificate to the list of trusted certificates in one of the following ways:

- Indicate the path to the certificate file. The **Browse** button opens the standard file selection window. Indicate the path to the file that contains the certificate, in DER or PEM format.
- Copy the contents of the certificate file to the **Enter certificate details** field.

Traffic interception exclusions window

The table contains the settings of connections that the application excludes from traffic interception:

- **Remote IP address** is the IP address to which the traffic excluded from interception is going to or from which it is coming from (depending on the direction of traffic).
- **Destination port** is a port on a protected device (in an inbound traffic interception exclusion) or a port on a remote device (in an outbound traffic interception exclusion).
- **Traffic direction** is the direction of traffic in the connection: inbound or outbound.

You can add, edit, or delete exclusions.

Traffic interception exclusion window

In this window, you can add a traffic interception exclusion. To do this, you need to specify the following connection settings:

- **Remote IP address** is the IPv4 or IPv6 address of the remote device. Depending on the traffic direction, traffic coming from the specified IP address (exclusion for inbound traffic) or traffic going to the specified IP address (exclusion for outgoing traffic) is excluded.
- **Destination port**, depending on traffic direction:
  - Port on the protected device (exclusion for inbound traffic). Traffic to this port from remote devices is excluded from interception.
  - Port on the remote device (exclusion for outbound traffic). Traffic to this port from the protected device is excluded from interception.
- **Traffic direction** is the direction of traffic in the excluded connection. You can configure an exclusion for inbound traffic or for outbound traffic.

In an exclusion, you may specify an IP address of the remote device without a port or a destination port without an IP address.

> If you specify only the IP address of the remote device in an exclusion for inbound traffic (without specifying a port on the protected device), all traffic from the remote device is excluded from interception. We recommend configuring this exclusion only for traffic from devices that you trust.

Monitored ports

Network ports settings

Setting	Description
Monitor all network ports	If this option is selected, the application monitors all network ports.
Monitor selected network ports only	If this option is selected, the application monitors only the network ports specified in the table. This option is selected by default.
Network ports settings	This table contains network ports monitored by the application if the **Monitor selected network ports only** option is selected. The table contains two columns: • **Port** – monitored port. • **Description** – description of the monitored port. By default, the table displays a list of network ports that are usually used for the transmission of mail and network traffic. The list of network ports is included in the application package. You can add, edit, and delete items in the table.

Global exclusions

In the Administration Console, you can configure global exclusions in the policy properties (**General settings** → **Global exclusions**).

The **Excluded mount points** group of settings contains a **Configure** button. Clicking this button opens the **Excluded mount points** window.

The list in the window contains the paths to the excluded mount points. By default, the list is empty.

You can add, edit, and delete items in the list.

Mount point path window

Mount point settings

Setting	Description
File system, access protocol, and path	The settings block lets you set the location of the mount point. In the drop-down list of file systems, you can select the type of file system where the directories that you want to add to scan exclusions are located: • **Local**: local mount points. • **Mounted**: remote directories mounted on the device using the Samba or NFS protocol. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
	If **Mounted** is selected in the drop-down list of file systems, you can select the remote access protocol in the drop-down list on the right: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. • **Custom**: all the resources of the device file system specified in the field below.
	If **Local** is selected in the drop-down list of file systems, then in the input field you can enter a path to a mount point that you want to exclude from file operation interception. You can use masks to specify the path. Mount points must be specified in the same way as they are displayed in the `mount` command output.
Filesystem name	The field for entering the name of the file system where the directories that you to exclude from file operation interception are located. The field is available if the **Mounted** type is selected in the drop-down list of file systems and the **Custom** item is selected in the drop-down list on the right.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Excluding process memory from scans

In the Administration Console, you can configure excluding process memory from scans in the policy properties (**General settings** → **Excluding process memory**).

Clicking **Configure** under **Exclude process memory from scans** opens a window where you can create a list of exclusions.

The list in the **Exclude process memory from scans** window contains the paths to processes that the application excludes from process memory scanning. You can use masks to specify the path. By default, the list is empty.

You can enable the merging of the list of exclusions when inherited by child policies. To merge the list items, select the **Merge inherited values** check box in the **Exclude process memory from scans** window. If the check box is selected, items in the list of the parent policy are displayed in child policies, and items can be added to the list of the child policy. If the check box is cleared, the list items are not merged when inheriting policy settings. This check box is cleared by default.

Useful articles

How to specify masks

You can use the `*` (asterisk) character to create a file or directory name mask.

You can indicate a single `*` character to represent any set of characters (including an empty set) preceding the `/` character in the file or directory name. For example, `/dir/*/file` or `/dir/*/*/file`.

You can indicate two consecutive `*` characters to represent any set of characters (including an empty set and the `/` character) in the file or directory name. For example, `/dir/**/file*/` or `/dir/file**/`.

The `**` mask can be used only once in a directory name. For example, `/dir/**/**/file` is an incorrect mask.

You can use a single `?` character to represent any one character in the file or directory name.

Backup

In the Administration Console, you can manage Backup settings in the policy properties (**General settings** → **Storage settings**) and in managed device properties (**Managed devices** → **Devices** tab → device properties window → **Applications** section → application properties window → **Storage settings**).

Backup settings

Setting	Description
Store objects no longer than (days)	This check box enables or disables the storage period limit (in days) for the objects in the Backup storage. Possible values: 0–10000. If 0 is specified, the period for storing objects in the Backup storage is unlimited. Default value: 30.
Limit the size of Backup to (MB)	This check box enables or disables the maximum Backup storage size (in megabytes). Possible values: 1–4000. If the check box is cleared, the size of Backup is unlimited. This check box is cleared by default.

Detection of applications that hackers can use to harm

In the Administration Console, you can detection of legitimate applications that intruders can use to compromise devices or data in the policy properties (**General settings** → **Application settings**, **Scan settings** section).

Application detection settings that intruders can use to compromise devices or data

Setting	Description
Detect legitimate applications that intruders can use to compromise devices or data	This check box enables or disables the detection of legitimate applications that could be used by hackers to harm computers or data of users. This check box is cleared by default.

Interception of file operations

In the Administration Console, you can configure the file operation interception mode in the policy properties (**General settings** → **Application settings**, **File operations interception mode** section).

File operation interception settings

Setting	Description
Block access to files during scans	This check box enables or disables the blocking of access to files while they are being scanned by the File Threat Protection and Device Control components, the Execution prevention action, and the Removable Drives Scan task. This check box is selected by default. If the check box is cleared, access to any file is allowed for the duration of the scan, and the scan runs in asynchronous mode.

Sending information to Kaspersky Security Center storage

In Kaspersky Security Center, you can enable or disable the transfer of data about files in Backup, quarantined files, unprocessed files, and connected devices to the Kaspersky Security Center storage.

The general list of files quarantined by Kaspersky applications on client devices is kept in Kaspersky Security Center and is also available in the Administration Console (**Advanced** → **Repositories** → **Quarantine**).

A general list of files placed in Backup by Kaspersky applications on client devices is generated in Kaspersky Security Center and is available in the Administration Console (**Advanced** → **Repositories** → **Backup**).

Information about unprocessed files is displayed in the list of active threats in the Administration Console (**Advanced** → **Repositories** → **Active threats**).

Information about devices installed on or connected to the client device is displayed in the list of equipment in the Administration Console (**Advanced** → **Repositories** → **Hardware**). Data is transferred if Device Control is enabled.

Information about applications detected on the client device is also displayed in the list of applications in the Administration Console (**Advanced** → **Application management** → **Applications registry**). Data is transferred if Application Control is enabled.

Enabling and disabling the transfer of data in the Administration Console

In the Administration Console, you can enable or disable data transfer to the Administration Server in policy properties (**General settings** → **Storage settings**, **Transfer data to the Administration Server**) or in the properties of the managed device (**Managed devices** → **Devices** tab → device properties window → **Applications** section → application properties window → **Storage settings**, **Transfer data to the Administration Server** section).

Clicking **Configure** in the **Transfer data to the Administration Server** section opens the **Data transfer settings**, in which you can enable or disable the transfer of data to the Administration Server.

Settings for transferring data to the Administration Server

Setting	Description
About files in Quarantine	This check box enables or disables the transfer of data about quarantined files to the Administration Server. This check box is selected by default.
About files in Backup	This check box enables or disables the transfer of data about files in Backup to the Administration Server. This check box is selected by default.
About unprocessed files	This check box enables or disables sending notifications about the files, which were not processed during the scan, to the Administration Server. This check box is selected by default.
About installed devices	This check box enables or disables the transfer of data about devices installed on a client device or connected to it, to the Administration Server. This check box is selected by default.
About applications found on the device	This check box enables or disables the sending of the list of applications that the Inventory task discovers on the client device to the Administration Server. This check box is selected by default.

System event interception

In the Administration Console, you can configure system event interception in the policy properties (**General settings** → **OS interaction settings**, **System event interception settings** section).

The settings are applied only on devices running an operating system that supports the fanotify technology.

System event interception settings

Setting	Description
Interception mechanism	The system event interception mechanism used by the application: • **Fanotify technology** (default). If this option is selected, the application uses the fanotify technology for system event interception. • **Updatable kernel module**. If this option is selected, the application uses the updatable kernel module for system event interception.
If the updatable kernel module fails to start	Action that the application performs if the updatable kernel module fails to start: • **Use fanotify** (default). If this option is selected, the application switches to the fanotify technology for system event interception. • **Disable system event interception** If the application does not use system event interception, real-time file scanning is not performed, and the protection level of the device is reduced. This option is available if the **Updatable kernel module** interception mechanism is selected.

Additional telemetry settings

In the Administration Console, you can manage additional telemetry settings in the policy properties (**General settings** → **OS interaction settings**, **Additional telemetry settings** section).

Additional telemetry settings

Setting	Description
Telemetry source	The source that Kaspersky Endpoint Security uses to collect telemetry: • **Use only eBPF** means only the eBPF technology is used for obtaining telemetry. • **Use eBPF and auditd** (default) means the eBPF technology and auditd service are used to get telemetry.

Setting	Description
Using auditd	The mode of the auditd service: • **Use AuditD in exclusive mode** (default) means Kaspersky Endpoint Security uses the auditd service in exclusive mode. • **Non-exclusive mode** means the auditd service is used in non-exclusive mode. This setting is applied only if **Telemetry source** is set to **Use eBPF and auditd**.

Light Agent mode

In the Administration Console, you can manage settings for connecting Light Agent to SVMs in the policy properties (**Light Agent mode**).

Connection to the Integration Server

The settings described in this section apply only if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments.

A connection to the Integration Server is required if you want Light Agents to receive information about the SVM through the Integration Server, or if you want to protect the connection between the Protection Server and the Light Agent.

This window displays the current settings for connecting Light Agents to the Integration Server: address and port for connecting. The **Edit** button opens the **Connection to the Integration Server** window, where you can configure the connection to the Integration Server.

Connection to the Integration Server window

In this window, you can specify or change the settings for connecting Light Agents to the Integration Server.

Integration Server connection settings

Setting	Description
Address	IP address in IPv4 format or fully qualified domain name (FQDN) of the device on which the Integration Server is installed. If the device on which Kaspersky Security Center Administration Console is installed is part of a domain, the field indicates the domain name of this device by default. If the device on which the Kaspersky Security Center Administration Console is installed is not part of a domain or the Integration Server is installed on another device, the field must be filled in manually. If the address is specified as a NetBIOS name, localhost or 127.0.0.1, connection to the Integration Server completes with an error.
Port	Port for connecting to the Integration Server. By default, port 7271 is specified.

If a Linux-based high-availability cluster of Integration Servers is deployed in your infrastructure, you need to specify the address and port of the load balancer as the address and port for connecting to the Integration Server. For more details, refer to the Kaspersky Security for Virtualization Light Agent Help.

Verify Integration Server certificate window

This window appears if the SSL certificate received from the Integration Server contains an error or is not trusted.

You can click the link in the window to view the details of the received certificate.

If you encounter problems with an SSL certificate, we recommend to make sure that the data transmission channel you are using is secure.

To continue connecting to the Integration Server, click the **Ignore** button. The received certificate will be installed as a trusted certificate on the device where the Kaspersky Security Center Administration Console is installed.

Authentication on the Integration Server window

This window appears if the device hosting the Kaspersky Security Center Administration Console does not belong to a domain or your account does not belong to the KLAdmins local or domain group or to the local administrator group.

Specify the password of the Integration Server administrator (password of the `admin` account) and click the **OK** button.

It is recommended to make sure that the password complexity and anti-bruteforce mechanisms ensure that the password cannot be guessed within 6 months.

After connecting to the Integration Server with administrator rights, the policy automatically receives the password of the `agent` account, which is used to connect Light Agents to the Integration Server.

SVM discovery settings

The settings described in this section apply only if Kaspersky Endpoint Security is used in Light Agent mode.

In this window, you can select the method that Light Agents use to discover SVMs available to connect to.

SVM discovery settings

Setting	Description
Use the Integration Server	If this option is selected, Light Agent connects to Integration Server to get a list of SVMs available for connection and their details. If you want to use the Integration Server, you need to configure the settings for connecting Light Agents to the Integration Server.
Use a custom list of SVM addresses	If this option is selected, you can specify a list of SVMs that Light Agents managed by this policy can connect to. Light agents will only connect to SVMs specified in the list.
List of SVMs	The list of IP addresses in IPv4 format or fully qualified domain names (FQDNs) of the SVMs to which Light Agents covered by the policy can connect. Click **Add** to open a window in which you can specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line. Specify only fully qualified domain names (FQDNs) that map to a single IP address. Using a fully qualified domain name that corresponds to multiple IP addresses can lead to errors in the application. You can delete addresses selected in the list by clicking the **Delete** button. The list of SVM addresses is displayed if the **Use a custom list of SVM addresses** option is selected.

If you select the **Use a custom list of SVM addresses** option, the Light Agent is using the extended SVM selection algorithm, and large infrastructure protection mode is enabled on an SVM (for more information, see the Kaspersky Security for Virtualization Light Agent Help), then connecting a Light Agent to this SVM is only possible if the SVM path is ignored. In the **SVM selection algorithm** section, you need to set the **SVM path** setting to **Ignore**. If any other value is set, Light Agents will not be able to connect to the SVM.

SVM connection tag

In this window, you can enable the Light Agent to use tags and assign a tag that the Light Agent will use to connect.

Make sure that the use of connection tags is also configured in the Protection Server settings: For more information, see the Help for Kaspersky Security for Virtualization Light Agent. Light Agents assigned a tag can only connect to SVMs that are allowed to connect to Light Agents with that tag.

Settings for using connection tags

Setting	Description
Use connection tag	The check box enables or disables the use of SVM connection tags by the Light Agent.
Tag	A tag that is assigned to Light Agents. For a tag, you can enter a text string up to 255 characters long. You can use any character except the `;` character. The field is available if the **Use connection tag** check box is selected.

SVM selection algorithm

In this window, you can specify which SVM selection algorithm Light Agents must use, and configure the settings for using the extended SVM selection algorithm.

SVM selection algorithm

Setting	Description
Use the standard SVM selection algorithm	If this option is selected, after installing and running on a virtual machine, the Light Agent selects an SVM to connect to that is local to Light Agent. For more details, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent. If no local SVMs suitable for connection are to be found, the Light Agent selects an SVM to which the least number of Light Agents is connected, regardless of the position of the SVM in the virtual infrastructure. This option is selected by default.
Use the extended SVM selection algorithm	If this option is selected, you can use the **SVM path** slider to specify how the SVM's location in the virtual infrastructure will be taken into account when determining whether the SVM is local relative to the Light Agent. The Light Agent will only be able to connect to SVMs that are local. You can also specify that the SVM path in the virtual infrastructure should not be taken into account when selecting an SVM to connect to. When selecting an SVM, Light Agents consider the number of Light Agents connected to the SVM to ensure an even distribution of Light Agents among the SVMs available to connect to.

Setting	Description

SVM path	Allows you to specify the type of SVM path in the virtual infrastructure, which is taken into account when selecting SVMs for connection:
	• **Hypervisor**. The Light Agent selects an SVM to connect to that meets the criteria (depending on the type of virtual infrastructure):
	  • The SVM is deployed on the same hypervisor as the virtual machine with the Light Agent installed (in a virtual infrastructure on the Microsoft Hyper-V platform, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, or Basis Dynamix Standard).
	  • The SVM is located in the same server group as the virtual machine with the Light Agent installed (in a virtual infrastructure running on the OpenStack or VK Private Cloud platform).
	  • The SVM is located on the same node as the virtual machine with the Light Agent installed (in a virtual infrastructure Basis Dynamix Enterprise).
	  If there are no SVMs available for connection on the same hypervisor or in the same Server Group where the virtual machine with the Light Agent is located, the Light Agent does not connect to the SVM.
	• **Cluster**. The Light Agent selects an SVM to connect to that meets the criteria (depending on the type of virtual infrastructure):
	  • The SVM is deployed in the same hypervisor cluster as the virtual machine with the Light Agent installed (in a virtual infrastructure on the Microsoft Hyper-V platform, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, or Basis Dynamix Standard).
	  • The SVMs are deployed in the same OpenStack project as the virtual machine with the Light Agent installed (in a virtual infrastructure running on the OpenStack platform or VK Private Cloud).
	  • The SVM is located in the same zone as the virtual machine with the Light Agent installed (in a virtual infrastructure Basis Dynamix Enterprise).
	  If there are no SVMs available for connection in the same hypervisor cluster or within the same OpenStack project where the virtual machine with the Light Agent is located, the Light Agent does not connect to the SVM.
	• **Data center**. The Light Agent selects an SVM to connect to that meets the criteria (depending on the type of virtual infrastructure):
	  • The SVM is deployed in the same data center as the virtual machine with the Light Agent installed (in a virtual infrastructure on the Microsoft Hyper-V platform, XenServer, VMware vSphere, KVM, Proxmox VE, Basis, HUAWEI FusionSphere, Nutanix Acropolis, ALT Virtualization Server, Astra Linux, Numa vServer, or Basis Dynamix Standard).
	  • The SVM is located in the same Availability Zone as the virtual machine with the Light Agent installed (in a virtual infrastructure running on the OpenStack platform or VK Private Cloud).
	  • The SVM is located in the same data center as the virtual machine with the Light Agent installed (in a virtual infrastructure Basis Dynamix Enterprise).
	  If there are no SVMs available for connection in the same data center or Availability Zone where the virtual machine with the Light Agent is located, the Light Agent does not connect to the SVM.
	• **Ignore**. When selecting an SVM, the Light Agent does not consider its location.
	The **Hypervisor** option is selected by default.
	The option is available if the **Use the extended SVM selection algorithm** option is selected.

If a Light Agent uses the extended SVM selection algorithm and a list of SVM addresses is selected as the SVM discovery method, and large infrastructure protection mode is enabled on an SVM (for more information, see the Kaspersky Security for Virtualization Light Agent Help), then connecting a Light Agent to this SVM is only possible if the SVM path is ignored. You must set the **SVM path** setting to **Ignore**. If any other value is set, Light Agents will not be able to connect to the SVM.

Protecting the connection

In this window, you can enable encryption of the data transmission channel between the Light Agent and the Protection Server

Make sure that encryption of the data transmission channel between the Light Agent and the Protection Server is enabled in the Protection Server settings on the SVM. For more details, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

Connection protection settings

Setting	Description
Encrypt data channel between Light Agent and the Protection Server	Use encryption to protect the connection between Light Agents and Protection Servers. If the check box is selected, an encrypted connection is established between the Light Agent, which is managed by policy, and the Protection Server on the SVM that the Light Agent is connecting to. A Light Agent for which connection protection is enabled can only connect to an SVM on which connection protection is enabled or an unprotected connection to the Protection Server is allowed. If the check box is cleared, an unprotected connection is established between the Light Agent and the Protection Server on the SVM that the Light Agent is connecting to. This check box is cleared by default.

Known issues and limitations

Limitations of the application

Kaspersky Endpoint Security is not supported in the following cases:

- On OSnova operating systems in the closed software environment mode and in the hardened kernel mode.
- On operating systems based on Red Hat Enterprise Linux, with the IMA subsystem.
- On operating systems based on Red Hat Enterprise Linux, in FIPS mode.
- On Ubuntu operating systems and operating systems based on SUSE Linux Enterprise Server, with the AppArmor mandatory access control system.
- With Grsecurity security systems (on all operating systems).
- When the seccomp mechanism is used (on all operating systems).
- When WSL1 and WSL2 technologies are used (on all operating systems).
- When certain file system mount options are used (for example, noexec, nosuid).
- When Kaspersky Endpoint Security is installed inside a container.

Detection and Response solutions may not work correctly on virtual machines created from an image with Kaspersky Endpoint Security for Linux installed. When integrating with Detection and Response solutions, a unique ID (Sensor ID) of the computer is used. The application generates this ID as part of the initial installation, and it is retained even after the application is uninstalled. When cloning an image, the virtual machine inherits the Sensor ID, which may cause Detection and Response solutions to identify multiple virtual machines as the same device.

Limitations of the application on certain architectures

The application has limitations when running on the following processor architectures:

Elbrus

- Light Agent mode: not supported.
- EDR agent mode: not supported.
- BadUSB Attack Prevention: does not work.
- Exploit Prevention: does not work.
- Web Threat Protection: heuristic analysis is not available when scanning web pages for phishing links.

- Kaspersky Endpoint Detection and Response Optimum integration: Not working.
- Kaspersky Endpoint Detection and Response Expert (cloud) integration: Not working.
- Kaspersky Endpoint Detection and Response (KATA) integration: Not working.
- Kaspersky Managed Detection and Response integration: Not working.
- Sandbox: does not work.
- KUMA Integration: Not working.
- Container Scan: does not work.
- Updatable kernel module: Not supported.
- Management graphical user interface: users cannot submit files for scanning in Sandbox because the Sandbox component is not supported.

Limitations of the application on some operating systems

The application has limitations when running on the following operating systems:

Astra Linux Special Edition RUSB.10015-01 (operational update 1.5)

- BadUSB Attack Prevention: Not working, because the systemd-logind service is missing from operating system.
- The limitation on CPU resource usage for the Malware Scan, Critical Areas Scan, Inventory, and Container Scan tasks does not work on "4.2.0-23-generic" cores.

CentOS 5.2 and 5.4

- Behavior Detection: the component is not guaranteed to work correctly because synchronous interception process starts is not available.
- Mail Threat Protection: Not working.
- Web Threat Protection: does not work, because there is no support for the TProxy mechanism.
- Network Threat Protection: does not work, because there is no support for the TProxy mechanism.
- Anti-Cryptor: does not work, because there is no support for the TProxy mechanism.
- BadUSB Attack Prevention: Not working, because the systemd-logind service is missing from operating system.
- Container Scan: does not work because the operating system does not support containers.
- Device Control: ReadOnly mode for devices works only if the device was connected after activating the mode in the application. For devices connected before this mode was activated, the access mode remains unchanged.

- Application Control: does not work because there is no support of the fanotify technology that is necessary for synchronous interception of process start.
- Firewall Management: does not work, because there is no support for adding chains to iptables.
- Web Control: does not work, because there is no support for the TProxy mechanism.
- Updatable kernel module: Not supported.
- Network Isolation: does not work, because there is no support for the TProxy mechanism.
- Execution prevention for objects does not work because there is no synchronous interception of process start.
- Kaspersky Endpoint Detection and Response Optimum integration: Not working.
- Kaspersky Endpoint Detection and Response Expert (cloud) integration: Not working.
- Kaspersky Endpoint Detection and Response (KATA) integration: The eBPF telemetry source is unavailable.
- Kaspersky Managed Detection and Response integration: The auditd telemetry source is unavailable.
- Graphical user interface: does not work, because the libxcb library is missing from the operating system.
- Kaspersky Security Center Network Agent: requires additional device configuration. See the Kaspersky Security Center Help.
- Installation/Removal: The application is not compatible with SELinux in these version of the operating system. Possible solution: put SELinux in non-blocking mode (permissive mode), disable SELinux, or manually configure SELinux.
- Malware Scan: In operating systems with glibc versions earlier than 2.11, files located in directories with a path length longer than 4096 characters are not disinfected or deleted.
- The limitation on CPU resource usage for the Malware Scan, Critical Areas Scan, Inventory, and Container Scan tasks is not working.
- Light Agent mode is not supported, therefore the KSVLA_MODE, SERVER_MODE, VDI_MODE settings are not applicable when installing the application.
- Application operation in EDR Agent mode is not supported.
- The application is not supported in Kaspersky Security Center Cloud Console.
- The application does not support file systems based on the FUSE technology.
- Statistics of the most frequently scanned files is not collected.
- In some cases, telemetry transmitted as part of integration with Kaspersky Endpoint Detection and Response (KATA) may contain incomplete information about events from the system event logs.

CentOS 6.4 and 6.6

- Behavior Detection: the component is not guaranteed to work correctly because synchronous interception process starts is not available.
- Web Threat Protection: interception of IPv6 traffic does not work.

- Network Threat Protection: interception of IPv6 traffic does not work.
- Anti-Cryptor: interception of IPv6 traffic does not work.
- BadUSB Attack Prevention: Not working, because the systemd-logind service is missing from operating system.
- Container Scan: does not work because the operating system does not support containers.
- Application Control: does not work because there is no support of the fanotify technology that is necessary for synchronous interception of process start.
- Firewall Management: IPv6 rules of the Firewall do not work.
- Web Control: interception of IPv6 traffic does not work.
- Updatable kernel module: Not supported.
- Execution prevention for objects does not work because there is no synchronous interception of process start.
- Kaspersky Endpoint Detection and Response Optimum: the threat development chain does not represent network activity because there is no TProxy support. Only telemetry events about file operations are available. Object execution prevention does not work because synchronous interception of process start is not available.
- Kaspersky Endpoint Detection and Response Expert (cloud) integration: Not working.
- Kaspersky Endpoint Detection and Response (KATA) integration: The eBPF telemetry source is unavailable.
- Kaspersky Managed Detection and Response integration: The auditd telemetry source is unavailable.
- Kaspersky Security Center Network Agent: requires additional device configuration. See the Kaspersky Security Center Help.
- Installation/Removal: The application is not compatible with SELinux in these version of the operating system. Possible solution: put SELinux in non-blocking mode (permissive mode), disable SELinux, or manually configure SELinux.
- Malware Scan: In operating systems with glibc versions earlier than 2.11, files located in directories with a path length longer than 4096 characters are not disinfected or deleted.
- Application operation in Light Agent mode and EDR Agent mode is not supported.
- The application is not supported in Kaspersky Security Center Cloud Console.
- Statistics of the most frequently scanned files is not collected.
- In some cases, telemetry transmitted as part of integration with Kaspersky Endpoint Detection and Response (KATA) may contain incomplete information about events from the system event logs.

Limitations related to the values of the ptrace setting

The values of the operating system's `kernel.yama.ptrace_scope` setting may affect Kaspersky Endpoint Security:

- 1 (limited ptrace). A process can connect only to processes that it has started. Special permission is required to connect to other processes. The functionality of the application is limited as follows:
  - The Behavior Detection component cannot obtain the environment parameters of processes.
  - On operating systems with a kernel version later than 5.7, the Application Control component cannot read command line arguments and environment variables of processes because reading /proc/<pid>/syscall and /proc/<pid>/mem is prohibited. On operating systems with kernel version 5.0, the Application Control component cannot function properly.
  - The process memory and kernel memory scan does not work in scan tasks, since reading /proc/<pid>/mem is prohibited.
  - YARA scanning of process memory is not guaranteed because reading /proc/<pid>/mem is not allowed.
- 2 (administrative ptrace). Only processes with CAP_SYS_PTRACE privileges (usually root) can use ptrace or gain access to a process in /proc (/proc/<pid>/mem). Troubleshooting is limited in that crash dumps do not work for user processes (such as kesl-control and kesl-gui), although dumps do work for the kesl process itself.
- 3 (ptrace prohibited): ptrace fully prohibited at operating system level. The functionality of the application is limited as follows:
  - Crash dumps do not work for the kesl process or user processes (such as kesl-control and kesl-gui).
  - The Behavior Detection component cannot obtain the environment parameters of processes.
  - The Application Control component is not supported.
  - Because the /proc/<pid>/mem directory cannot be read:
    - Scanning of process memory and kernel memory in scan tasks does not work.
    - The Get memory dump and Get process memory dump tasks do not work when integrating with Detection and Response solutions.
    - YARA scans of process memory are not guaranteed to work in mandatory access control mode when integrated with Kaspersky Endpoint Detection and Response Expert (on-premises).

Limitations of the updatable kernel module

The updatable kernel module does not support the following varieties and versions of kernels:

Ubuntu

- `*-kvm`
- `*-gkeop 5.15.0-100[1234] (bionic/jammy)`
- `focal 5.10.0-1002-oem`
- `noble 6.8.0-1014-ibm`
- `*-realtime`
- `*-uc-*`
- `kinetic 5.18.0-100(1|2)-(ibm|gcp|oracle)`

Astra

- `6.1.90-1-generic-*, 6.6.28-1-generic-*`
- `*-hardened`

Debian

- `*-rt`
- `5.14.0-1-(cloud-amd64|amd64)-5.14.6-2`
- `6.1.0-36-(cloud-amd64|amd64)-6.1.139-1`
- `6.5.0-5-*amd64-6.5.13-1`
- `6.6.*`

RED OS 7.3.

- `kernel-ml-5.14.9-1.el7`

RED OS 8.0

- `6.6.26-1.red80`
- `6.6.34-1.red80`
- `6.6.51-1.red80`
- `6.6.76-1.red80`
- `6.6.6-1.red80`

Limitations on the use of eBPF technology

To use eBPF technology for intercepting network traffic, you need a Linux kernel 4.18 or later, compiled with the following options:

- `CONFIG_DEBUG_INFO_BTF=y` or `m` (support for eBPF with BTF)
- `CONFIG_KPROBES= y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_FSNOTIFY=y`

To use eBPF for sending telemetry when integrating with Detection and Response solutions, you need a Linux kernel 4.18 or later, compiled with the following options:

- `CONFIG_BPF=y`
- `CONFIG_BPF_SYSCALL=y`
- `CONFIG_TRACEPOINTS=y`
- `CONFIG_KPROBES=y`
- `CONFIG_KPROBES_ON_FTRACE=y`
- `CONFIG_KRETPROBES=y`
- `CONFIG_HAVE_SYSCALL_TRACEPOINTS=y`
- `CONFIG_FTRACE=y`
- `CONFIG_FUNCTION_TRACER=y`
- `CONFIG_DYNAMIC_FTRACE=y`
- `CONFIG_DYNAMIC_FTRACE_WITH_REGS=y`
- `CONFIG_FTRACE_SYSCALLS=y`
- `CONFIG_KPROBE_EVENTS=y`
- `CONFIG_FSNOTIFY=y`

Special considerations

- The application cannot be used in Light Agent mode and in EDR Agent mode at the same time.
- In operating systems with auditd 3.0.7 and Linux kernel 4.18, using the Behavior Detection component may result in the freezing of the application and ssh connections.
- On Kylin Desktop V10 SP1 2303 operating systems, the Behavior Detection component may freeze the operating system. To resolve this issue, we recommend updating the kernel of the operating system.

Special considerations for Light Agent mode

If Kaspersky Endpoint Security is used in Light Agent mode:

- Application management using Kaspersky Security Center Cloud Console and the graphical user interface is not available.
- The use of cloud databases is not supported.
- Kaspersky Endpoint Security interacts with KSN servers using a KSN proxy server. Direct communication with KSN is not supported.
- The use of a proxy server for the application is not supported when connecting to the Integration Server, SVMs, or KSN servers.

Special considerations for EDR Agent mode

If Kaspersky Endpoint Security is being used in EDR Agent mode, only a limited subset of application component and tasks is available. After installation, the application settings are as follows:

- Kaspersky Endpoint Detection and Response Expert (cloud) integration is not supported.
- The following components that provide integration with Detection and Response solutions are fully manageable:
  - EDR Expert (on-premises)
  - NDR (KATA)

  These components are disabled by default, you need to enable them for the application to work in EDR Agent mode. You can manage integration settings, including the functionality of Execution prevention of objects.
- Access to files is not blocked during the scan: the **Block access to files during scans** check box is cleared (`FileBlockDuringScan=No`). This setting can be modified, but is not applied on the protected device.

- The File Threat Protection and Anti-Cryptor protection components are available in reduced functionality mode: when a threat is detected, these components do not attempt to disinfect or delete malicious objects, block access or application activity, but only send information about threat detection to Integration Servers that provide integration with Detection and Response solutions.

  You can enable or disable File Threat Protection and Anti-Cryptor and manage component settings, except for Action on threat detection. The following settings are not applied on the protected device:

  - File Threat Protection: **Action on threat detection** is **Skip** (`ActionOnThreat=Skip`).
  - Anti-Cryptor: **Action on encryption detection** is **Inform** (`ActionOnDetect=Notify`).

- The Behavior Detection component is fully manageable.
- All other protection and control components are disabled and cannot be managed.

When integrated with Kaspersky Endpoint Detection and Response Expert (on-premises) or with Kaspersky Endpoint Detection and Response (KATA), as part of a threat response action, Kaspersky Endpoint Security can control the launch of executable files and scripts on the device. The functionality of Execution prevention for objects is available with the following limitations:

- If a script is launched from an interpreter, the application does not control the launch of the script.
- The application does not control the opening of office software files on the device.

Contact Technical Support

If you do not find a solution to your problem in the application documentation or other sources of information about the application, it is recommended to contact Technical Support. Technical Support specialists will answer any of your questions about installing and using Kaspersky Endpoint Security.

Kaspersky provides support for every version of Kaspersky Endpoint Security during the life cycle of the version (refer to the application life cycle page). Before contacting Technical Support, please read the support rules.

You can contact Technical Support in one of the following ways:

- Visit Technical Support website.
- Submit a request to Kaspersky Technical Support from the Kaspersky CompanyAccount portal.

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount is a portal for companies that use Kaspersky applications. Kaspersky CompanyAccount allows organizations using Kaspersky applications to contact Kaspersky Technical Support via email requests. On the portal, you can create new requests, monitor their progress and keep a history of request processing.

Register all employees of your organization under a single account on Kaspersky CompanyAccount. This will let you centrally manage electronic requests to Kaspersky and control the access of your users to Kaspersky CompanyAccount.

The Kaspersky CompanyAccount portal is available in the following languages:

- English
- Spanish
- Italian
- German
- Polish
- Portuguese
- Russian
- French
- Japanese

To learn more about Kaspersky CompanyAccount, visit the Kaspersky CompanyAccount Technical Support website.

Obtaining information for Technical Support

After you inform Kaspersky Technical Support specialists about the problem, they may ask you to send a *trace file* or *dump file*.

Technical Support specialists may also need additionally information about the operating system and running processes on the device, as well as detailed reports on the operation of application components.

While diagnosing the problem, Technical Support specialists may ask you to change the application settings to:

- activate functionality to receive advanced diagnostic information;
- perform more detailed configuration of individual application components that cannot be performed through the standard user interface;
- change settings for storing received diagnostic information;
- to configure the capture and storage of network traffic in a file.

Technical Support specialists will tell you all the information required to perform these actions (the sequence of steps, the settings to change, configuration files, scripts, advanced command line capabilities, debugging modules, special utilities, etc.), as well as the body of information received for diagnostic purposes. The received advanced diagnostic information is stored on the user device. This information is not automatically sent to Kaspersky.

The steps listed above should be performed only with the guidance of Technical Support specialists based on instructions they provide. Independently changing application files using means not described in the application documentation or not recommended by Technical Support specialists may lead to poor performance and failures in the application and operating system, reduced protection, as well as inaccessible and corrupted data.

How to enable and configure trace file creation

A *trace file* tracks the step-by-step execution of application commands and detects at what stage of application operation the error occurs.

Application trace files are not generated by default. You can enable or disable trace file creation and select the tracing level on the command line in general application settings or in the graphical user interface.

If you are managing the Kaspersky Endpoint Security application through Kaspersky Security Center, you can manage the trace settings of the application in the Kaspersky Endpoint Security policy settings using the Web Console or the Administration Console.

How to manage trace settings in the Web Console

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.

3. Select the **Application settings** tab.

4. Go to the **General Settings** → **Technical Support** section and look under **Trace settings**.

5. If you want to change the directory in which the application's trace files are saved by default, specify the directory for storing the trace files in the **Trace folder path** field. Default value: /var/log/kaspersky/kesl. Root privileges are required to access the default trace files directory. If you specify a different directory, make sure that only the root has read and write permissions to this directory (`700` or `rwx--------` permissions).

6. If necessary, specify the maximum size of an application trace file (in megabytes) in the **Maximum trace file size (MB)** field. Default value: 500.

7. If necessary, specify the maximum number of application trace files in the **Maximum number of trace files** field. Default value: 10.

8. Save your changes.

9. Restart the application to apply the trace settings.

How to manage trace settings in the Administration Console

1. In the tree of the Kaspersky Security Center Administration Console, in the **Managed devices** folder, open the folder with the name of the administration group that includes the required devices.

2. In the workspace, select the **Policies** tab.

3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.

   You can also open the policy properties window by using the **Properties** item in the policy context menu or by clicking the **Configure policy settings** link located to the right of the list of policies in the section with the policy settings.

4. Go to the **General settings** → **Application settings** section.

5. Under **Trace and dump settings**, click **Configure**.

6. This opens the **Trace and dump settings** window.

7. If you want to change the directory in which the application's trace files are saved by default, specify the directory for storing the trace files in the **Path to the trace file directory** field. Default value: /var/log/kaspersky/kesl. Root privileges are required to access the default trace files directory. If you specify a different directory, make sure that only the root has read and write permissions to this directory (`700` or `rwx-------` permissions).

8. If necessary, specify the maximum size of an application trace file (in megabytes) in the **Maximum trace file size (MB)** field. Default value: 500.

9. If necessary, specify the maximum number of trace files that the application can create in the **Maximum number of trace files** field. Default value: 10.

10. Click **OK** in the **Trace and dump settings** window.

11. Click **Apply**.

12. Restart the application to apply the trace settings.

How to enable tracing and manage trace settings on the command line

On the command line, you can configure tracing using the `TraceLevel`, `TraceFolder`, `TraceMaxFileCount`, and `TraceMaxFileSize` settings in the general application settings. You can change the values of the settings with the help of command line switches or a configuration file that contains all general application settings.

To create a trace file and configure trace settings on the command line:

1. Enable the creation of a trace file and select a tracing level:

   ```
   kesl-control --set-app-settings TraceLevel=Detailed | MediumDetailed | NotDetailed
   ```

   Where:

   - `Detailed` – Generate a detailed trace file.
   - `MediumDetailed` – Generate a trace file that contains informational messages and error messages.
   - `NotDetailed` – Generate a trace file that contains error messages.

2. If you want to change the directory in which the application's trace files are saved by default, specify the directory for storing the trace files:

   ```
   kesl-control --set-app-settings TraceFolder=<path to trace files directory>
   ```

   Where `<path to trace files directory>` is the path to the directory in which trace files are stored. Default value: /var/log/kaspersky/kesl. Root privileges are required to access the default trace files directory. If you specify a different directory, make sure that only the root has read and write permissions to this directory (`700` or `rwx--------` permissions).

3. If necessary, specify the maximum number of trace files:

   ```
   kesl-control --set-app-settings TraceMaxFileCount=<number of application trace files>
   ```

   Where `<number of application trace files>` is the maximum number of application trace files. Possible values: 1 to 10000 Default value: 10.

4. If necessary, specify the maximum size of an application trace file (in megabytes):

   ```
   kesl-control --set-app-settings TraceMaxFileSize=<size of an application trace file>
   ```

   Where `<size of an application trace file>` is the maximum size of a trace file in megabytes. Possible values: 1 to 1000 Default value: 500.

After changing the values of the `TraceFolder`, `TraceMaxFileCount`, or `TraceMaxFileSize` settings, you need to restart the application.

```
To disable the trace file creation, run the following command:
```

```
kesl-control --set-app-settings TraceLevel=None
```

How to enable tracing and manage trace settings in the graphical interface

To create a trace file and configure its level of detail, you need a user with the Administrator role (admin).

1. Open the main window of the application graphical interface.
2. In the lower part of the main application window, click the **Support** button.

   The **Support** window opens.
3. Click the **Tracing** link to open the **Tracing** window
4. In the **Level** drop-down list, select the level of detail for the trace file:

   - **Diagnostic (300)** – only error messages.
   - **Informational (700)** – informational and error messages.
   - **Debug (800)** – detailed trace file.

   We recommend that you clarify the required level of detail with a Kaspersky Technical Support specialists. The default setting is **Diagnostic (300)**.
5. Click the **Enable** button to start tracing.
6. Reproduce the situation which caused the problem.
7. Click the **Disable** button to stop tracing.

Created trace files are stored in /var/log/kaspersky/kesl/ directory.

You can also enable and configure the creation of Watchdog server trace files.

How to enable tracing and manage the Watchdog server trace settings on the command line

On the command line, you can configure the Watchdog server tracing using the `WdTraceLevel` settings in the general application settings. You can change the values of the settings using command line options or a configuration file that contains all general application settings.

```
Create the Watchdog server trace file and configure the trace settings from the command line

kesl-control --set-app-settings WdTraceLevel=Detailed | MediumDetailed | NotDetailed | Product
```

Where:

- `Detailed` – Generate a detailed trace file.
- `MediumDetailed` – Generate a trace file that contains informational messages and error messages.

- `NotDetailed` – Generate a trace file that contains error messages.
- `Product` – set the value equal to the value of the `TraceLevel` setting in general application settings. If `TraceLevel=None`, a trace file is not generated.

```
Disable the creation of the Watchdog server trace file and configure the trace settings from the command line

kesl-control --set-app-settings WdTraceLevel=None
```

By default, the created trace files are stored in the /var/log/kaspersky/kesl/ directory. Access to this directory requires root privileges. You can specify a different directory for storing trace files. If you specify a different directory, make sure that only the root has read and write permissions to this directory (`700` or `rwx--------` permissions).

Trace files of the graphical interface and the kesl-control command line utility are stored in the /var/log/kaspersky/kesl-user directory. To enable the creation of these trace files, you need to set the LFS_ENABLE_ALL_COMPONENTS_LOGGING environment variable.

To store trace files, the application needs disk space in addition to the disk space listed in minimum hardware requirements.

Trace files are stored on the device as long as the application is in use, and are deleted permanently when the application is removed. Trace files are not sent to Kaspersky automatically.

Trace files are saved in a human-readable format. It is recommended to protect information from unauthorized access before sending it to Kaspersky.

MMC management plug-in trace files

If you use the Administration Console to manage Kaspersky Endpoint Security, information about events that occur while the administration MMC plug-in is running can be saved to the Kaspersky Endpoint Security MMC plug-in trace file on the device where the Administration Server is installed. The file name contains the application version number, file creation date and time, and process identifier (PID). This file contains information about the events that occur during MMC plug-in operation, in particular, about the operation of policies and tasks.

MMC plug-in trace files are not generated by default. You can use registry keys to create the MMC plug-in trace file. Contact Technical Support representatives for detailed information on how to create trace files.

All created trace files of the MMC plug-in are located in the folder specified by the user during registry key configuration.

Management web plug-in trace files

If you use the Web Console to manage Kaspersky Endpoint Security, information about events that occur while the administration web plug-in is running can be written to the web plug-in trace files.

Trace files for the web plug-in are created automatically if logging of Web Console activities is enabled in Web Console Installation Wizard (for more details, refer to the Kaspersky Security Center Help).

Trace files of the web plug-in are stored in the Web Console installation folder in the "logs" subfolder.

Application trace file contents

Trace files contain the following general data:

- Event time.
- Number of the thread of execution.
- Application component that caused the event.
- Degree of event severity (informational event, warning, critical event, error).
- A description of the event involving command execution by a component of the application and the result of execution of this command.

Trace files may store the following information in addition to general data:

- The statuses of the application components and their operational data.
- Data on user activity in the application.
- Data on the hardware installed on the device.
- Data about all operating system objects and events, including information about user activity.
- Data contained in the objects of the operating system (for example, the contents of files that may contain any user personal data).
- Network traffic data (for example, the contents of the entry fields on a website, which may include bank card information or any other sensitive data).
- Data received from Kaspersky servers (such as the version of the application databases).
- Data received from KATA servers, OSMP servers, NDR servers, and servers that provide interaction with Sandbox.
- Data on consumed CPU resources.
- Data on consumed RAM resources.
- Data about file read and write operations by applications.
- Data on the amount of cached information required for the application to work.

Contents of management plug-in trace files

Trace files of management plug-ins contain the following general data:

- Event time.
- Number of the thread of execution.
- Application component that caused the event.
- Degree of event severity (informational event, warning, critical event, error).
- A description of the event involving command execution by a component of the application and the result of execution of this command.

In addition to general data, trace files of management plug-ins may contain the following information:

- Personal data, including the last name, first name, and middle name, if such data is part of the path to files.
- The name of the account used to log in to the operating system if the user account name is part of a file name.

How to enable and configure dumping

A *dump file* contains all information about the working memory of Kaspersky Endpoint Security processes at the time of creating the dump

> Dump files may contain personal data. It is recommended to protect information from unauthorized access before sending it to Kaspersky.

No dump files are generated by default. You can enable or disable dumping in case of application failures.

If you are managing the Kaspersky Endpoint Security application through Kaspersky Security Center, you can enable or disable dumping and configure it in the Kaspersky Endpoint Security policy settings using the Web Console or the Administration Console.

If you use the command line to manage the application, you can enable or disable dumping via the general application settings.

The maximum number of dump files is limited.

> Depending on the operating system settings, user dump files may not be created. Make sure that the system kernel is configured using `sysctl kernel.yama.ptrace_scope=0`.

How to enable and configure dumping in the Web Console

To enable and configure dumping in the Web Console:

1. In the main window of the Web Console, select **Asset management** → **Policies**.
2. Click the name of the Kaspersky Endpoint Security policy.

   The policy properties window opens.
3. Select the **Application settings** tab.
4. Go to the **General Settings** → **Technical Support**, section, **Debug information**.
5. If you want a dump file to be generated when the application crashes, enable the **Dump writing ENABLED** toggle switch.

6. If you want to change the directory in which dump files of the kesl process are saved by default, specify the directory for storing dump files in the **Code dump path** field. Default value: /var/opt/kaspersky/kesl/common/dumps. Root privileges are required to access the default dump file directory. If you specify a different directory, make sure that only the root has read and write permissions to this directory (`700` or `rwx--------` permissions).

7. Save your changes.

How to enable and configure dumping in the Administration Console

To enable and configure dumping in the Administration Console:

1. In the tree of the Kaspersky Security Center Administration Console, in the **Managed devices** folder, open the folder with the name of the administration group that includes the required devices.

2. In the workspace, select the **Policies** tab.

3. In the list of policies, select the required policy and double-click it to open the **Properties: <Policy name>** window.

   You can also open the policy properties window by using the **Properties** item in the policy context menu or by clicking the **Configure policy settings** link located to the right of the list of policies in the section with the policy settings.

4. Go to the **General settings** → **Application settings** section.

5. Under **Trace and dump settings**, click **Configure**.

6. This opens the **Trace and dump settings** window.

7. If you want a dump file to be generated when the application crashes, select the **Create a dump file if the application crashes** check box.

8. If you want to change the directory in which dump files of the kesl process are saved by default, specify the directory for storing dump files in the **Path to the dump file directory** field. Default value: /var/opt/kaspersky/kesl/common/dumps. Root privileges are required for access to the default dump file directory (`700` or `rwx--------` permissions). If you specify a different directory, make sure that only the root has read and write permissions to this directory.

9. Click **OK** in the **Trace and dump settings** window.

10. Click **Apply**.

How to enable and configure dumping on the command line

On the command line, you can enable, disable, and configure dumping using the `CoreDumps` and `CoreDumpsPath` settings from general application settings.

To enable and configure dumping:

1. Run the following command to enable dumping:

```
kesl --set-app-settings CoreDumps=Yes
```

2. If you want to change the directory where dump files are saved, specify the path to the directory in the `CoreDumpsPath` setting.

   ```
   kesl --set-app-settings CoreDumpsPath=<path to directory with dump files>
   ```

   Where `<path to directory with dump files>` is the path to the directory where the dump files are stored. Default value: /var/opt/kaspersky/kesl/common/dumps. Root privileges are required for access to the default dump file directory (`700` or `rwx--------` permissions). If you specify a different directory, make sure that only the root has read and write permissions to this directory.

To disable dumping, run the following command:

```
kesl --set-app-settings CoreDumps=No
```

If you have enabled dumping, by default, dump files are stored in the following directories:

- /var/opt/kaspersky/kesl/common/dumps (dump files of the kesl process)
- /var/opt/kaspersky/kesl/common/dumps-user (dump files of user processes)

Root privileges are required to access the default dump file directory. You can specify a different directory for storing the dump files of the kesl process. If you specify a different directory, make sure that only the root has read and write permissions to this directory (`700` or `rwx--------` permissions).

To store dump files, the application needs disk space in addition to the disk space listed in minimum hardware requirements.

Dump files are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed. Dump files are not sent to Kaspersky automatically.

Remote device diagnostics using Kaspersky Security Center

In Kaspersky Security Center you can perform remote diagnostics of client devices. The remote diagnostics procedure lets you remotely run the following operations:

- Enable or disable tracing.
- Change the trace level.
- Download trace files.
- Download a remote application installation log.
- Download system event (syslog) logs.
- Start, stop, and restart applications.

Remote diagnostics in the Web Console

If you use the Web Console to manage Kaspersky Endpoint Security, remote diagnostics of a client device is done in the remote diagnostics window.

To open the remote device diagnostics window for a device:

1. In the main window of the Web Console, select **Assets (Devices)** → **Managed devices**.

   The list of managed devices opens.

2. Select a device that you want to diagnose remotely and click the <device name> link.

   The device properties window opens.

3. On the **Advanced** tab, select the **Remote diagnostics** section.

In the device remote diagnostics window, you can view the remote installation log.

To view the remote installation log on a device, do as follows:

1. Open the remote device diagnostics window.

2. On the **Event logs** tab, under **Trace files** block, click **Remote installation logs**.

   The **Device trace event logs** window opens.

For more information about the remote diagnostics, see the Kaspersky Security Center Help.

Remote diagnostics using the Administration Console

If you use the Administration Console to manage Kaspersky Endpoint Security, remote diagnostics is done using the special Kaspersky Security Center remote diagnostics utility automatically installed on the device together with the Administration Console.

To open the main window of the remote diagnostics utility, do as follows:

1. In the Administration Console tree, in the **Managed devices** folder, select the administration group containing the necessary device.

2. In the workspace, select the **Devices** tab.

3. In the list of managed devices, select the device to which you want to connect the remote diagnostics utility, and select **External tools** → **Remote diagnostics** in the device context menu.

   The main window of the **Kaspersky Security Center remote diagnostics utility** opens.

You can use the remote device diagnostics utility to view the remote installation log.

To view the remote installation log on a device, do as follows:

1. Open the main window of the remote diagnostics utility.

2. Configure the options for connecting the utility to the device if needed. In the main window of the remote diagnostics utility, click the **Log in** button.

3. In the window that opens, in the objects tree, select the **Remote installation logs** folder.

For more information about the remote diagnostics utility, refer to Kaspersky Security Center Help section.

Appendices

This section provides information that complements the primary Help text.

Appendix 1. Configuration files and default application settings

The following configuration files are used for managing Kaspersky Endpoint Security:

- Configuration files that contain the initial configuration settings of the application:
- Preset configuration files generated automatically during the initial configuration of the application and containing the options set during the initial configuration. These settings are applied at run time.
- Configuration files that you can create with Kaspersky Endpoint Security management commands. These configuration files may contain task settings and other application settings. You can modify these files and import into the application to modify the corresponding options.

Rules for editing task configuration files

When editing a configuration file, adhere to the following rules:

- Specify all mandatory settings in the configuration file. You can specify individual task settings without a file using the command line.
- If a setting belongs to a certain section, specify it only in this section. You can specify the settings in any order within the one section.
- Enclose the names of sections in square brackets [ ].
- Specify the values of settings in the `< setting name >=< setting value >` format (spaces between the setting name and its value are not processed).

  Example:
  ```
  [ScanScope.item_0000]
  AreaDesc=Home
  AreaMask.item_0000=*doc
  Path=/home
  ```

  Space and tab characters are ignored before the first quotation mark and after the last quotation mark of a string value, and at the beginning and end of a string value that is not enclosed in quotation marks.

- If you need to specify several values for a setting, repeat the setting the same number of times as the number of values that you want to specify.

  Example:
  ```
  AreaMask.item_0000=*xml
  AreaMask.item_0001=*doc
  ```

- Be case-sensitive when entering values for the following types of settings:
  - Names (masks) of scanned objects and excluded objects.
  - Names (masks) of threats.

  The remaining setting values are not case-sensitive.
- Specify Boolean setting values as follows: `Yes` / `No`.
- Use quotation marks to enclose string values containing a space character (for example, names of files and directories and their paths, expressions containing the date and time in the format "YYYY-MM-DD HH:MM:SS").

  You can enter the remaining values with or without quotation marks.

  Example:
  `AreaDesc=" Scanning of email databases "`

  A single quotation mark in the beginning or end of a string is considered an error.

Initial configuration files

You can specify initial configuration settings of the application using a configuration file:

- If you are installing the application using Kaspersky Security Center, in the archive for remote application installation, you can find the autoinstall.ini config file. You can specify settings in this file before creating the installation package. Kaspersky Security Center applies these settings during application installation.
- If you install the application using the command line, you need to create the configuration file and specify the path to it when starting the Initial Configuration Wizard. You can copy the structure of this file from the autoinstall.ini configuration file.

In the post-installation configuration file, you can specify the settings shown in the table below. The set of applicable settings depends on the application usage mode. Default values are specified for the autoinstall.ini file.

Which values are valid for some settings depends on whether you are installing remotely via Kaspersky Security Center or on the command line.

To change a setting in the configuration file, specify its value in the <setting name>=<value> format.

Example

```
UPDATER_SOURCE=KLServers
```

Setting	Description	Values

[CustomSettings] section	Fine-tuning the application during remote installation. Lets you change some of the settings in the kesl.ini file and also the tracing level.
	
	You can configure the application using this section only during the initial installation.
	
	If the `[CustomSettings]` section duplicates the settings of the autoinstall.ini file, the autoinstall.ini settings are applied to the application.
		• Any setting in the kesl.ini configuration file in the <setting section>.<setting name>=<value> format
		Example
		`[CustomSettings]`
		`General.Locale=ru_RU.utf8`
		`Network.ProxyRouteTable=202`
		`Watchdog.MaxMemory=20MB`
		• `TraceLevel`, detail level of the application trace files:
		  • `Detailed` – Generate a detailed application trace file.
		  • `MediumDetailed` – Generate an application trace file that contains informational messages and error messages.
		  • `NotDetailed` – Generate an application trace file that contains error messages.
		  • `None` (default value) – Do not generate an application trace file.
		• `WdTraceLevel`, detail level of the Watchdog server trace files:
		  • `Detailed` to generate a detailed Watchdog server trace file.
		  • `MediumDetailed` to generate a Watchdog server trace file that contains informational messages and error messages.
		  • `NotDetailed` to generate a Watchdog server trace file that contains error messages.
		  • `None` not to generate a Watchdog server trace file.
		  • `Product` (default value) to set the value equal to the `TraceLevel` value.

EULA_AGREED	Required setting. Acceptance of the terms of the End User License Agreement.	`Yes` (default) – accept the terms and conditions of the End User License Agreement. `No` – do not accept the terms and conditions of the End User License Agreement. The application installation will be terminated.
PRIVACY_POLICY_AGREED	Required setting. Acceptance of the terms of the Privacy Policy.	`Yes` (default) – accept the terms and conditions of the Privacy Policy. `No` – do not accept the terms and conditions of the Privacy Policy. The application installation will be terminated.

Setting	Description	Values
USE_KSN	Required setting. Enabling Kaspersky Security Network usage: To enable the use of KSN, the terms of the Kaspersky Security Network Statement must be accepted. If Kaspersky Endpoint Security is used in Standard mode and you have enabled the use of KSN, the application's cloud mode is automatically enabled. In this mode, Kaspersky Endpoint Security uses a lightweight version of the malware databases.	`Yes` – accept the terms of the Kaspersky Security Network Statement and enable the use of KSN. `No` – (default value) do not accept the terms and conditions of the Kaspersky Security Network Statement. Opting out of the KSN does not abort the application installation process.
LOCALE	The locale used for the application events sent to Kaspersky Security Center. The locale of the graphical interface and the application command line is taken from the `LANG` environment variable. If the application does not support this localization, it defaults to the English localization.	Locale in RFC 3066 format. Possible values: • `de_DE.UTF-8` – German • `en_US.UTF-8` – English (USA) • `es_MX.UTF-8` – Spanish (Mexico) • `fr_FR.UTF-8` – French • `ja_JP.UTF-8` – Japanese • `pt_BR.UTF-8` – Portuguese (Brazil) • `ru_RU.UTF-8` – Russian • `zh_TW.UTF-8` – Chinese Traditional • `zh_CN.UTF-8` – Chinese Simplified If the `LOCALE` setting is not specified, the operating system locale is used. If the application cannot detect the locale of the operating system or this locale is not supported, English (en_US.UTF-8 in RFC 3066 format) is used to localize events.
INSTALL_LICENSE	In the autoinstall.ini configuration file: the activation code for adding a license key to the application. In the command line configuration file, you can also specify the path to the key file to add a license key to the application. This setting applies only if the application is used in standard mode.	`<activation code>` if you want to activate the application using an activation code when installing via Kaspersky Security Center or on the command line. `<full path to key file>` if you want to activate the application using a key file during installation on the command line. `None` if you do not want to activate the application during installation, for example, if you are installing the application in an isolated network segment without internet access.

Setting	Description	Values
UPDATER_SOURCE	Update source for databases and application modules. This parameter is applied only if the application is used in standard mode or in EDR agent mode.	`SCServer` – use the Kaspersky Security Center Administration Server as the update source. `KLServers` (default) – use Kaspersky servers as the update source. `<update source address>` as a local directory (for example, /home/bases) or a remote HTTP or HTTPS server (for example, http://example.com/bases/).
PROXY_SERVER	Address of the proxy server used to connect to the Internet. This parameter is applied only if the application is used in standard mode or in EDR agent mode.	Address of the proxy server in one of the following formats: • `[<connection protocol>://] <address of the proxy server>:<port>`, if no authentication is required to connect to the proxy server; • `[<connection protocol>://] [<user name>: [<password>]@]<address of the proxy server>:<port>`, if authentication is required when connecting to the proxy server. When specifying an IPv6 address, enter it in square brackets. Connecting to a proxy server over HTTPS is not supported.
UPDATE_EXECUTE	Start the application database update task during the initial configuration. This parameter is applied only if the application is used in standard mode or in EDR agent mode.	`Yes` (default value) – start the update task. `No` – do not start update task.
KERNEL_SRCS_INSTALL	Automatically compile the kernel module when starting File Threat Protection. This setting only applies to operating systems that do not support fanotify.	`Yes` (default) – compile the kernel module when File Threat Protection starts. `No` – do not compile the kernel module.
USE_GUI	Installing and using the graphical interface of the application. This parameter is applied only if the application is used in standard mode or in EDR Agent mode.	`Yes` – install and use the application's graphical interface (the files for installing the graphical interface must be added to the installation package). `No` (default) – do not use the graphical interface.

Setting	Description	Values
GROUP_CLEAN	Required setting. Automatically removing users from the kesladmin and keslaudit privileged groups before installing the application.	`Yes` - Remove users from the privileged groups. If the value is `Yes` and there is no nogroup group, the installation will fail and you will be prompted to manually remove users from privileged groups. `No` (default) – Do not remove users from the privileged groups.
ADMIN_USER	A user assigned the administrator role (admin). The Administrator role allows managing application settings and task settings in the graphical interface of the application and on the command line without using the `sudo` command.	
CONFIGURE_SELINUX	Automatic configuration of SELinux for working with Kaspersky Endpoint Security.	`Yes` (default value) – automatically configure SELinux to work with Kaspersky Endpoint Security. `No` – do not perform automatic SELinux configuration.
DISABLE_PROTECTION	Disabling the functional components of the application after installation. An installation with components disabled can be convenient, for example, if you need to reproduce a problem with the application and create a trace file. If you enable the necessary components after installing the application with `DISABLE_PROTECTION=Yes`, the enabled components will continue to work after the application is restarted.	`Yes` - Disable protection components and scan tasks when the application is started after installation. `No` - Do not disable protection components and scan tasks when the application is started after installation.
ENDPOINT_AGENT_MODE	Using Kaspersky Endpoint Security in EDR agent mode. This setting is not applicable to devices with an Elbrus CPU.	`Yes` – Kaspersky Endpoint Security is being used in the EDR Agent mode to support Kaspersky Detection and Response solutions working together with third-party anti-virus solutions on protected devices. `No` (default value) – Kaspersky Endpoint Security is used in standard mode or in Light Agent mode (see the KSVLA_MODE setting).
EDR_EXPERT_CLOUD_MODE	Select the mode of the Endpoint Detection and Response Expert component. This setting applies only if the application is used in standard mode. This setting is not applicable to devices with an Elbrus CPU.	`Yes` means the application uses the Kaspersky Endpoint Detection and Response Expert (cloud) integration. `No` (default value) means the application uses the Kaspersky Endpoint Detection and Response Expert (on-premises) integration.

Setting	Description	Values
KSVLA_MODE	Using Kaspersky Endpoint Security in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.	`Yes` - Kaspersky Endpoint Security is used in Light Agent mode (as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent). `No` (default value) – Kaspersky Endpoint Security is used in standard mode or in EDR Agent mode (see the ENDPOINT_AGENT_MODE setting).
SERVER_MODE	The role of the protected virtual machine (server or workstation). The setting is applied only if the application is used in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.	`Yes` - the protected virtual machine is used as a server. `No` - the protected virtual machine is used as a workstation.
VDI_MODE	Enabling VDI protection mode to optimize application performance on temporary virtual machines. The setting is applied only if the application is used in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.	`Yes` – enable VDI protection mode. This is recommended if you are installing Kaspersky Endpoint Security on a virtual machine template that will be used to create temporary virtual machines. `No` – do not enable VDI protection mode.
INTERCEPTOR_MODE	The system event interception mechanism used by Kaspersky Endpoint Security: This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.	`UseFanotify` (default) – use the fanotify technology to intercept system events. `UseUpdatableKernelModule` – use an updatable kernel module to intercept system events.

Setting	Description	Values
INTERCEPTOR_FALLBACK_STRATEGY	What the application does if the updatable kernel module fails to start. This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.	`FallbackToFanotify` (default) – switch to fanotify for system event interception. `FallbackToLimitedMode` – do not use system event interception. As a result, real-time file scanning is not performed, and the protection level of the device is reduced.
INTERCEPTOR_APPLY_STRATEGY	If the application switches to using the updatable kernel module, the application must be restarted to start the module. This setting lets you specify if you want the application to be restarted automatically or if you prefer to restart the application manually. This setting applies only when installing via Kaspersky Security Center. This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.	`RestartServiceAutomatically` (default value) automatically restarts the application to start the updatable kernel module. `RestartServiceManually` starts the updatable kernel module after the application is restarted manually by the user. We recommend automatically restarting the application to switch to using the updatable kernel module. Starting the updatable kernel module manually after restarting the application can lead to application errors.
ENABLE_TRACES_ON_FIRST_STARTUP	Create a trace file when the application is started for the first time after installation. To create a trace, a kesl_startup.log file is automatically created in the /var/log/kaspersky/kesl/ directory. The size limit for regular application trace files does not apply to this file. Tracing stops after five minutes or after the File Threat Protection task is started.	`Yes` – create a trace file when the application is started for the first time after installation. `No` (default value) – Do not create a trace file at first start of the application.

Setting	Description	Values
AK_FORCED_PACKAGE_MANAGER_OPERATIONS_AS_FALLBACK	Use the application installation mode that ignores the errors of the package manager. This mode can be used if the application could not be installed normally. This setting applies only when installing via Kaspersky Security Center. Changing the default values is only recommended under the supervision of the Technical Support specialists and based on their instructions.	`No` (default value) to install the application normally. `Yes` to install the application while ignoring system errors.
AK_REMOVE_PARTIALLY_INSTALLED_PACKAGE	Automatically remove the application installation package if it was only partially installed. Disable this setting if the application could not be installed normally. This setting applies only when installing via Kaspersky Security Center. Changing the default values is only recommended under the supervision of the Technical Support specialists and based on their instructions.	`Yes` (default value) to remove a partially installed application installation package. `No` to install the application ignoring the partially installed package.
AK_PACKAGE_MANAGER_DEBUG_LOG_OUTPUT	Enable debug logs for package managers. This setting can be used if the application could not be installed normally. This setting applies only when installing via Kaspersky Security Center. Changing the default values is only recommended under the supervision of the Technical Support specialists and based on their instructions.	`Yes` to enable debug logs for package managers. `No` (default value) not to enable debug logs for package managers.

Initial configuration settings in the installation package

You can specify initial configuration settings for the application in the installation package that you are using to install the application using Kaspersky Security Center.

In Kaspersky Security Center Web Console, you can specify the initial configuration settings for Kaspersky Endpoint Security in the installation package properties on the **Settings** tab. The created installation packages are available in the main window of the Web Console in one of the following sections:

- **Device discovery and deployment** → **Deployment and assignment** → **Installation packages**.
- **Operations** → **Repositories** → **Installation packages**.

In the Kaspersky Security Center Administration Console, you can specify the initial configuration settings for Kaspersky Endpoint Security when creating an installation package or in the installation package properties, in the **Settings** section. The created installation packages are available in the tree of the Administration Console in the **Additional** → **Remote installation** → **Installation packages** folder.

The set of applicable settings depends on the application usage mode.

Initial configuration settings in the Web Console

Initial configuration settings

Setting	Description
Usage mode	• **Standard mode to protect workstations and servers** (default value). If this option is selected, the application is used as a stand-alone application for protecting Linux workstations and servers. • **Endpoint Detection and Response Agent**. If this option is selected, the application is used to support Kaspersky Detection and Response solutions working together with third-party anti-virus solutions on protected devices. • **Light Agent for protecting virtual environments**. If this option is selected, the application is used in Light Agent mode (as part of Kaspersky Security for Virtualization Light Agent). The EDR Agent mode and Light Agent mode are not available for devices with an Elbrus CPU.
Enable Endpoint Detection and Response Expert (cloud)	Select the check box to use the Endpoint Detection and Response Expert (cloud) integration. In Standard mode, the application supports integration with Endpoint Detection and Response Expert (cloud) and Endpoint Detection and Response Expert (on-premises). If this check box is cleared, integration with Endpoint Detection and Response Expert (on-premises) is used. This setting applies only if the application is used in standard mode This setting is not applicable to devices with an Elbrus CPU.

Setting	Description
Enable VDI protection mode	Select this check box to enable VDI protection mode. This is recommended if you are installing the application on a virtual machine template that will be used to create temporary virtual machines. This check box is cleared by default. The setting is applied only if the application is used in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.
The protected virtual machine is used as a server	The role of the virtual machine on which the application will be installed: server or workstation. By default, this check box is selected (the virtual machine is used in the virtual infrastructure as a server). The setting is applied only if the application is used in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.
Language of events in KSC	Localization language for application events sent to Kaspersky Security Center: • **System** (default) to use the operating system locale. If the application cannot detect the locale of the operating system or this locale is not supported, English is used to localize events. • One of the languages supported by Kaspersky Endpoint Security: English (USA), Spanish (Mexico), Chinese Traditional, Chinese Simplified, German, Portuguese (Brazil), Russian, French, Japanese. The locale of the graphical interface and the application command line is taken from the `LANG` environment variable. If the application does not support this localization, it defaults to the English localization.
Activate the application	Select this check box if you want to activate the application during installation. In the displayed field, enter the activation code. This check box is cleared by default. This setting applies only if the application is used in standard mode.
Update sources	Update source for databases and application modules. • **Kaspersky update servers** (default). • **Kaspersky Security Center**. • **Other source in the local or global network**. If you select this option, enter the address of the update source in the field that opens. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
Run database update task after installation	If this check box is selected, after the application is installed, the databases and application modules update task starts. This check box is selected by default. Clear this check box if you have added pre-downloaded application databases to the installation package. This parameter is applied only if the application is used in standard mode or in EDR agent mode.

Setting	Description
Specify the proxy server settings	Select this check box if you use a proxy server for internet access. In the displayed field, enter the proxy server address in one of the following formats: • `[<connection protocol>://]<address of the proxy server>:<port>`, if no authentication is required to connect to the proxy server; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, if authentication is required when connecting to the proxy server. When specifying an IPv6 address, enter it in square brackets. Connecting to a proxy server over HTTPS is not supported. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
Install kernel source code	If this check box is selected, starting File Threat Protection automatically starts the compilation of the kernel module on operating systems that do not support fanotify. This check box is selected by default. This setting only applies to operating systems that do not support fanotify. This setting is not applicable to devices with an Elbrus CPU.
Use the graphical user interface	Select this check box if you plan to install and use the application graphical interface. Files for installing the graphical interface must be added to the installation package. This check box is cleared by default. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
Specify a user with the admin role	Select this check box to specify the user to which you want to assign the admin role. The Administrator role allows managing application settings and task settings in the graphical interface of the application and on the command line without using the `sudo` command. In the displayed field, enter the user name.
Configure SELinux automatically	If this check box is selected, SELinux is automatically configured to work with Kaspersky Endpoint Security during the initial configuration of the application. This check box is selected by default.
Remove users from privileged groups	Select this check box to automatically remove users from the 'kesladmin' and 'keslaudit' privileged groups before installing the application. This check box is cleared by default. If the check box is selected and the 'nogroup' group does not exist, the installation fails and you are prompted to manually remove users from privileged groups.
Disable protection components and scan tasks for the first application startup after installation	Select this check box if, after completing the installation process, you want to run the application with protection components and scan tasks disabled. Installation with protection components disabled can be convenient, for example, to reproduce a problem in the operation of the application and create a trace file. If you enable the necessary components and tasks, the enabled components and tasks will continue to work after the application is restarted.
Enable tracing when the application is started for the first time after installation	Select the check box if you want to create a trace file when the application is started for the first time after installation. To create a trace, a kesl_startup.log file is automatically created in the /var/log/kaspersky/kesl/ directory. The size limit for regular application trace files does not apply to this file. Tracing stops after five minutes or after the File Threat Protection task is started.

Setting	Description
Interception mechanism	The system event interception mechanism used by the application: • **Fanotify technology** (default). If this option is selected, the application uses the fanotify technology for system event interception. • **Updatable kernel module**. If this option is selected, an updatable kernel module is installed during application installation. The application uses this module to intercept system events. This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.
If the updatable kernel module fails to start	The action the application performs if the updatable kernel module fails to start: • **Use fanotify** (default). If this option is selected, the application switches to the fanotify technology for system event interception. • **Disable system event interception** If the application does not use system event interception, real-time file scanning is not performed, and the protection level of the device is reduced. This option is available if the **Updatable kernel module** interception mechanism is selected. This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.
Enable package manager error ignoring mode	Select this check box to ignore package manager errors when installing the application. This check box is cleared by default. This setting can be used if the application could not be installed normally. We recommend that you enable this setting only under the supervision of Technical Support

Initial configuration settings in the Administration Console

Initial configuration settings

Setting	Description
Language of events in KSC	Localization language for application events sent to Kaspersky Security Center: • **System** (default) to use the operating system locale. If the application cannot detect the locale of the operating system or this locale is not supported, English is used to localize events. • One of the languages supported by Kaspersky Endpoint Security: English (USA), Spanish (Mexico), Chinese Traditional, Chinese Simplified, German, Portuguese (Brazil), Russian, French, Japanese. The locale of the graphical interface and the application command line is taken from the `LANG` environment variable. If the application does not support this localization, it defaults to the English localization.
Activation code	If you want to activate the application during installation, enter the activation code. This setting applies only if the application is used in standard mode.

Setting	Description
Select update source	Clicking the **Configure** button opens a window in which you can select the databases and application modules update source: • **Kaspersky update servers** (default value). • **Kaspersky Security Center**. • **Other source on the local or global network**. If you select this option, enter the address of the update source in the **Address** field. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
Run database update task after installation	If this check box is selected, after the application is installed, the databases and application modules update task starts. This check box is selected by default. Clear this check box if you have added pre-downloaded application databases to the installation package. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
Proxy server address	If you use a proxy server to access the internet, enter the address of your proxy server in one of the following formats: • `[<connection protocol>://]<address of the proxy server>:<port>`, if no authentication is required to connect to the proxy server; • `[<connection protocol>://][<user name>:[<password>]@]<address of the proxy server>:<port>`, if authentication is required when connecting to the proxy server. When specifying an IPv6 address, enter it in square brackets. Connecting to a proxy server over HTTPS is not supported. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
Install kernel source code	If this check box is selected, starting File Threat Protection automatically starts the compilation of the kernel module on operating systems that do not support fanotify. This check box is selected by default. This setting only applies to operating systems that do not support fanotify. This setting is not applicable to devices with an Elbrus CPU.
Use the graphical user interface	Select this check box if you plan to install and use the application graphical interface. Files for installing the graphical interface must be added to the installation package. This check box is cleared by default. This parameter is applied only if the application is used in standard mode or in EDR agent mode.
User with admin role	Name of the user to which you want to assign the admin role. The Administrator role allows managing application settings and task settings in the graphical interface of the application and on the command line without using the `sudo` command.
Configure SELinux automatically	If this check box is selected, SELinux is automatically configured to work with Kaspersky Endpoint Security during the initial configuration of the application. This check box is selected by default.
Remove users from privileged groups	Select this check box to automatically remove users from the 'kesladmin' and 'keslaudit' privileged groups before installing the application. This check box is cleared by default. If the check box is selected and the 'nogroup' group does not exist, the installation fails and you are prompted to manually remove users from privileged groups.

Setting	Description
Disable protection components and scan tasks when the application is started for the first time after installation	Select this check box if, after completing the installation process, you want to run the application with protection components and scan tasks disabled. Installation with protection components disabled can be convenient, for example, to reproduce a problem in the operation of the application and create a trace file. If you enable the necessary components and tasks, the enabled components and tasks will continue to work after the application is restarted.
Enable tracing when the application is started for the first time after installation	Select the check box if you want to create a trace file when the application is started for the first time after installation. To create a trace, a kesl_startup.log file is automatically created in the /var/log/kaspersky/kesl/ directory. The size limit for regular application trace files does not apply to this file. Tracing stops after five minutes or after the File Threat Protection task is started.
Application mode	This group of settings contains the **Configure** button. Clicking this button opens the **Application mode** window. In this window, you can select a mode for the application. • **Standard mode to protect workstations and servers** (default value). If this option is selected, the application is used as a stand-alone application for protecting Linux workstations and servers. • **Endpoint Detection and Response Agent**. If this option is selected, the application is used to support Kaspersky Detection and Response solutions working together with third-party anti-virus solutions on protected devices. • **Light Agent for protecting virtual environments**. If this option is selected, the application is used in Light Agent mode (as part of Kaspersky Security for Virtualization Light Agent). The EDR Agent mode and Light Agent mode are not available for devices with an Elbrus CPU.
Enable Endpoint Detection and Response Expert (cloud)	Select the check box to use the Endpoint Detection and Response Expert (cloud) integration. In Standard mode, the application supports integration with Endpoint Detection and Response Expert (cloud) and Endpoint Detection and Response Expert (on-premises). If this check box is cleared, integration with Endpoint Detection and Response Expert (on-premises) is used. This setting applies only if the application is used in standard mode. This setting is not applicable to devices with an Elbrus CPU.
The protected virtual machine is used as a server	The role of the virtual machine on which the application will be installed: server or workstation. By default, this check box is selected (the virtual machine is used in the virtual infrastructure as a server). The setting is applied only if the application is used in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.
Enable VDI protection mode	Select this check box to enable VDI protection mode. This is recommended if you are installing the application on a virtual machine template that will be used to create temporary virtual machines. This check box is cleared by default. The setting is applied only if the application is used in Light Agent mode. This setting is not applicable to devices with an Elbrus CPU.

Setting	Description
System event interception	This group of settings contains the **Configure** button. Clicking this button opens the **System event interception settings** window. In this window, you can select a system event interception mode, which you want application to use: • **Fanotify technology** (default value). If this option is selected, the application uses the fanotify technology for system event interception. • **Updatable kernel module**. If this option is selected, an updatable kernel module is installed during application installation. The application uses this module to intercept system events. This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.
If the updatable kernel module fails to start (**System event interception settings** window).	The action the application performs if the updatable kernel module fails to start: • **Use fanotify** (default). If this option is selected, the application switches to the fanotify technology for system event interception. • **Disable system event interception** If the application does not use system event interception, real-time file scanning is not performed, and the protection level of the device is reduced. This option is available if the **Updatable kernel module** interception mechanism is selected. This setting is applied only on devices running an operating system that supports the fanotify technology. This setting is not applicable to devices with an Elbrus CPU.
Enable package manager error ignoring mode	Select this check box to ignore package manager errors when installing the application. This check box is cleared by default. This setting can be used if the application could not be installed normally. We recommend that you enable this setting only under the supervision of Technical Support

Preset configuration files

After the initial configuration, the application creates the following configuration files:

- /var/opt/kaspersky/kesl/common/agreements.ini

  The agreements.ini configuration file contains settings related to the License Agreement, Privacy Policy, and Kaspersky Security Network Statement.

- /var/opt/kaspersky/kesl/common/kesl.ini

  The kesl.ini configuration file contains the settings described in the following table.

If necessary, you can edit the values of the settings in the kesl.ini file.

The default values in these files should be changed only under the supervision of Technical Support specialists and in accordance with their instructions.

To apply the changes made to the configuration file, restart the Kaspersky Endpoint Security application.

If a parameter is absent in the file or an incorrect parameter value is specified, the application will use the default value.

Settings of the kesl.ini configuration file

Setting	Description	Values
The **[General]** section contains the following settings:		
`Locale`	The locale used for the application events that Kaspersky Endpoint Security sends to Kaspersky Security Center. The locale of the graphical interface and the application command line is taken from the `LANG` environment variable. If the application does not support this localization, it defaults to the English localization.	The locale in the format specified by RFC 3066. If the `Locale` setting is not specified, the operating system locale is used. If the application cannot detect the locale of the operating system or this locale is not supported, English (en_US.UTF-8 in RFC 3066 format) is used to localize events.
`PackageType`	Format of the installed application package. We do not recommend changing the value of this setting manually. This value is filled in automatically during initial application configuration.	`rpm` – a RPM package is installed. `deb` – a DEB package is installed.
`UseFanotify`	Using the fanotify technology to intercept file operations. We do not recommend changing the value of this setting manually. This setting is specified during the initial configuration of the application. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` – the application uses the fanotify technology to intercept file operations. `false/no` – the fanotify technology is not used.
`KsvlaMode`	Using Kaspersky Endpoint Security in Light Agent mode. We do not recommend changing the value of this setting manually. This setting is specified during the initial configuration of the application. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` means that the application is being used in Light Agent mode. `false/no` – the application is used in Standard mode.

Setting	Description	Values
`EndpointAgentMode`	Using Kaspersky Endpoint Security in EDR agent mode. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` means that the application in EDR Agent mode. `false/no` – the application is used in Standard mode.
`KcsMode`	Use Kaspersky Endpoint Security as part of the Kaspersky Container Security solution as the File Threat Protection component. We do not recommend changing the value of this setting manually. This setting is used only by the Kaspersky Container Security solution. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` means the application is used as the File Threat Protection component in the Kaspersky Container Security solution. `false/no` (default) means the application is used in one of the Kaspersky Endpoint Security modes (standard mode, EDR Agent mode, or Light Agent mode).
`StartupTraces`	Enables generation of trace files at application startup.	`true/yes` – Create trace files at application startup. `false/no` (default value) – Do not create trace files at application startup.
`RevealSensitiveInfoInTraces`	Display information in trace files that may contain personal data (for example, passwords).	`true/yes` (default value) — display information in application trace files that may contain personal data. `false/no` (default value) — do not display information that may contain personal data in trace files.
`AsyncTraces`	Enables asynchronous tracing, in which information is logged to trace files in asynchronously.	`true/yes` – enable asynchronous tracing. `false/no` (default value) – do not enable asynchronous tracing.
`MinFreeDiskSpace`	The minimum amount of disk memory that will remain after writing a dump file, in megabytes.	Default value: 300.
`ScanMemoryLimit`	Limit on the application's use of RAM in megabytes.	Default value: 8192. We recommend specifying a `ScanMemoryLimit` lower than the `MaxMemory` setting to avoid using up all available memory for scan tasks and causing an application restart.
`MachineId`	The user's unique device ID.	The value of the setting is filled in automatically during installation of the application.
`SocketPath`	Path to a socket for a remote connection to, say, a graphical interface and the kesl-control utility.	Default value: /var/run/bl4control.
`MaxInotifyWatches`	Limit on the number of subscriptions to changes in files and directories (user watches) in /proc/sys/fs/inotify/max_user_watches. If the setting in the operating system is less than the `MaxInotifyWatches` setting, the application changes the operating system setting to the `MaxInotifyWatches` value.	Default value: 299987.
`MaxInotifyInstances`	Limit on the number of subscriptions to changes in files and directories for one user set in /proc/sys/fs/inotify/max_user_instances. If the setting in the operating system is less than the `MaxInotifyInstances` setting, the application changes the operating system setting to the `MaxInotifyInstances` value.	Default value: 4047.
`ExecEnvMax`	The number of environment variables that the application captures from the command call.	Default value: 50.

Setting	Description	Values
`ExecArgMax`	Number of arguments that the application captures from the exec call.	Default value: 20.
`AdditionalDNSLookup`	Indicates use of a public DNS. If there are errors accessing servers through the system DNS, the application uses a public DNS. This is needed for updating application databases and maintaining device security. The application will use the following public DNSes in this order: 1. Google Public DNS™ (8.8.8.8). 2. Cloudflare® DNS (1.1.1.1). 3. Alibaba Cloud® DNS (223.6.6.6). 4. Quad9® DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). The application's requests may contain domain addresses and the user's external IP address, since the application establishes a TCP/UDP connection with the DNS server. This information is necessary, for example, to check the certificate of a web resource when interacting via HTTPS. If the application is using a public DNS server, data processing rules are governed by the Privacy Policy of the corresponding service.	`true/yes` – Use a public DNS to access Kaspersky servers. `false/no` (default value) – Do not use a public DNS to access Kaspersky servers.
`PanicThreshold`	Maximum number of abnormal halts when using the updatable kernel module. When the specified value is reached, the application enters the "safe" mode, in which the updatable kernel module is not started. This setting is not applicable to devices with an Elbrus CPU.	Default value: 3.
`SafeMode`	Enabling the "safe" mode when using the updatable kernel module. In this mode, the application does not start the updatable kernel module. The "safe" mode is activated automatically if the application reaches the maximum number of abnormal halts specified in the `PanicThreshold` setting. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` means the "safe" mode of the application is enabled. `false/no` (default) means the "safe" mode of the application is disabled, the application operating normally.
`GetContainerName`	The following information about the container in included in telemetry when integrating with Kaspersky Managed Detection and Response: • Indication of the event occurring in a container • ID of the container namespace • Container name The container name is transmitted only if you have a license to use the Container Scan task and if the container has a sufficient lifetime. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` includes extended information about the container in telemetry when integrating with Kaspersky Managed Detection and Response. `false/no` does not include extended information about the container in telemetry when integrating with Kaspersky Managed Detection and Response.

Setting	Description	Values
`UseIncreasedXdrEventsCache`	Managing the event cache when integrated with Detection and Response solutions. There is a trade-off between high performance and RAM footprint.	`true/yes` (default value) minimizes disk I/O, but uses more RAM (100 MB). `false/no` uses less memory (about 5 MB) at the cost of more disk read and write operations.
`FastShutdown`	Fast shutdown of the kesl process when the application is stopped or restarted.	`true/yes` enables fast shutdown of the kesl process when the application is stopped. `false/no` (default value) disables fast shutdown of the kesl process when the application is stopped.
The **[Network]** section contains the following settings:		
`WtpFwMark`	A mark in the iptables rules for forwarding traffic to the application for processing by Web Threat Protection component. You may need to change this mark if a device with the application runs other software that uses the ninth bit of the TCP packet mask, and a conflict occurs.	A decimal value or hexadecimal number with the prefix 0x. Default value: 0x100. To avoid cyclical traffic scanning when the application is running on nodes used as part of distributed systems, such as Kubernetes, you need to change the values of the network packet marks using the higher bits. For example: 0x1000 or 0x10000 (the mark is limited to a 32-bit integer).
`NtpFwMark`	A mark in the iptables rules for forwarding traffic to the application for processing by Network Threat Protection component. You may need to change this mark if a device with the application runs other software that uses the ninth bit of the TCP packet mask, and a conflict occurs.	A decimal value or hexadecimal number with the prefix 0x. Default value: 0x200. To avoid cyclical traffic scanning when the application is running on nodes used as part of distributed systems, such as Kubernetes, you need to change the values of the network packet marks using the higher bits. For example: 0x2000 or 0x20000 (the mark is limited to a 32-bit integer).
`BypassFwMark`	A mark used to indicate packets created or scanned by the application, so that the application does not scan them again.	A decimal value or hexadecimal number with the prefix 0x. Default value: 0x400. To avoid cyclical traffic scanning when the application is running on nodes used as part of distributed systems, such as Kubernetes, you need to change the values of the network packet marks using the higher bits. For example: 0x4000 or 0x40000 (the mark is limited to a 32-bit integer).

Setting	Description	Values

`BypassNFlogMark`	Mark for packets that the application will ignore when scanning.	A decimal value or hexadecimal number with the prefix 0x.
		Default value: 0x800.
		Examples:
		Ignore all TCP traffic with the specified device:
		`iptables -t mangle -A PREROUTING -s <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -d <IP address (CIDR)> -p tcp -j MARK --set-xmark 0x800/0x800`
		Ignore HTTPS server traffic:
		`iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j MARK --set-xmark 0x800/0x800`
		`iptables -t mangle -A OUTPUT -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x800/0x800`
		To avoid cyclical traffic scanning when the application is running on nodes used as part of distributed systems, such as Kubernetes, you need to change the values of the network packet marks using the higher bits. For example: 0x8000 or 0x80000 (the mark is limited to a 32-bit integer).

`ProxyRouteTable`	Number of the routing table.	Default value: 101.
The **[ScannerImpactStats]** section contains the following settings:		
`CollectFileScanStatistics`	Enables the counting of file and process scanning statistics by the application.	`true/yes` (default value) enables the tallying of file and process scanning statistics. `false/no` disables the tallying of file and process scanning statistics.
`StatCollectionPeriod`	The time period during which the application collects statistics of scanned files and detected processes before saving the statistical information to the trace file and reports.	Default value: 10 minutes.
`StatCollectionCount`	The number of scanned files and detected processes counted by the application during the time interval specified by the `StatCollectionPeriod` parameter and that is included in the report and trace files.	Default value: 10.
`ReportStatAmount`	The number of records to be written to reports on the most frequently scanned files and processes for the day.	Default value: 20.
The **[Virtualization]** section contains the following settings:		
`ServerMode`	The role of the protected virtual machine on which Kaspersky Endpoint Security is used in Light Agent mode: server or workstation. We do not recommend changing the value of this setting manually. This setting is specified during the initial configuration of the application. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` – the protected virtual machine is used as a server. `false/no` – the protected virtual machine is used as a workstation.

Setting	Description	Values
`VdiMode`	Enables VDI protection mode when using the application in Light Agent mode. We do not recommend changing the value of this setting manually. This setting is specified during the initial configuration of the application. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` – VDI protection mode is enabled. `false/no` – VDI protection mode is disabled.
The **[Watchdog]** section contains the following settings:		
`TimeoutAfterHeadshot`	Maximum time to wait for the kesl process to complete from the moment the Watchdog server sends the HEADSHOT signal to the kesl process.	Default value: 2 minutes.
`StartupTimeout`	The maximum time to wait for the application to start (in minutes), after which the Watchdog server starts the procedure for restarting the kesl process.	Default value: 3 minutes.
`TimeoutAfterKill`	Maximum time to wait for the controlled kesl process to complete from the moment the Watchdog server sends the SIGKILL signal to the kesl process. If the kesl process does not finish before this time elapses, the action specified by the `--failed-kill` setting is performed.	Default value: 2 days.
`PingInterval`	The interval with which the application attempts to send a PONG message to the Watchdog server in response to a received PING message.	Default value: 2000 milliseconds.
`MaxRestartCount`	Maximum number of consecutive unsuccessful attempts to start the application.	Default value: 5.
`ActivityTimeout`	Maximum time interval during which the application should send a message to the Watchdog server. If a message is not received from the application within this time interval, the Watchdog server begins the procedure to restart the kesl process.	Default value: 2 minutes.
`ConnectTimeout`	The maximum timeout for the application's connection to the Watchdog server from the moment the kesl process starts. If the application does not establish a connection in this time interval, the Watchdog server begins the procedure to restart the kesl process.	Default value: 3 minutes.
`RegisterTimeout`	Maximum time from the moment the application connects to the Watchdog server to the moment the server receives a REGISTER message.	Default value: 500 milliseconds.
`TimeoutAfterShutdown`	Maximum time to wait for the kesl process to complete from the moment the Watchdog server sends the SHUTDOWN signal to the kesl process.	Default value: 2 minutes.

Setting	Description	Values
MaxMemory	Limit on the use of resident memory by the kesl process. If the kesl process uses more resident memory than this limit, the Watchdog server begins the procedure to restart the kesl process.	off – the resident set size is not limited. <value>% – a value between 1 and 100 percent of RAM. <value>MB – a value in megabytes. lowest/<value>%/<value>MB – the smaller of the percentage value and the absolute value in megabytes. highest/<value>%/<value>MB – the larger of the percentage value and the absolute value in megabytes. auto – up to 50% of available memory, but not less than 2GB and not more than 16GB. Default value: auto.
MaxVirtualMemory	Limit on the use of virtual memory by the kesl process. If the kesl process uses more virtual memory than this limit, the Watchdog server begins the procedure to restart the kesl process.	off (default value) – The virtual memory size is not limited. <value>MB – a value in megabytes.
MaxSwapMemory	Limit on the size of the swap file of the kesl process. If the swap file of the kesl process exceeds this limit, the Watchdog server begins the procedure to restart the kesl process.	off (default value) – The size of the swap file is not limited. <value>% – a value between 0 and 100 percent of RAM. <value>MB – a value in megabytes. lowest/<value>%/<value>MB – the smaller of the percentage value and the absolute value in megabytes. highest/<value>%/<value>MB – the larger of the percentage value and the absolute value in megabytes.
TrackProductCrashes	Enable the sending of device status from Kaspersky Endpoint Security to Kaspersky Security Center when the application is unstable.	true/yes enables the sending of device status information from Kaspersky Endpoint Security to Kaspersky Security Center. false/no (default) disables the sending of device status from Kaspersky Endpoint Security to Kaspersky Security Center.
ProductHealthLogFile	The path to the file used for application stability monitoring.	Default value: /var/opt/kaspersky/kesl/private/kesl_health.log.
WarnThreshold	Time interval (in seconds) in which the application must experience the specified number of abnormal halts before displaying a notification about unstable operation.	Default value: 3600 seconds.
WarnAfter_#_crash	The maximum number of abnormal halts of the application after which a notification about the unstable operation of the application is displayed.	Default value: 10. If the value is 0, an unstable application notification is not displayed.
WarnRemovingThreshold	Time interval (in seconds) after which the application's unstable status will be cleared.	Default value: 86400 seconds.
SyscallHangProbePeriod	The period with which the Watchdog server calls the open and execve system functions and increments the success counters for these functions.	Default value: 3 seconds.
SyscallHangCheckPeriod	The period with which the Watchdog server checks the success counters for the open and execve functions. If the value of the counters is unchanged after this time, the Watchdog server starts the procedure for restarting the kesl process.	Default value: 32 seconds.
DumpSuspendPeriod	The maximum time to wait for the creation of an application dump file, during which the Watchdog server suspends the checking of application activity. If the dump creation has not completed after this time, the Watchdog server starts the procedure for restarting the kesl process.	Possible values: 1–30 minutes. Default value: 2 minutes.

Setting	Description	Values
`TimeoutAfterCoredump`	The maximum duration for which the Watchdog server suspends the sending of other signals to the kesl process after sending the SIGTRAP signal as part of the abnormal process termination procedure.	Default value: 2 minutes. We recommend setting a `TimeoutAfterCoredump` greater than or equal to the `DumpSuspendPeriod`. You can use the following units to specify this setting: • `<n> day|days|d` for days • `<n> hour|hours|hr|h` for hours • `<n> minute|minutes|min|m` for minutes • `<n> second|seconds|sec|s` for seconds • `<n> [msec|ms]` for milliseconds If no unit is specified, the application interprets the value as milliseconds.
`TimeoutMaxCleanPeriod`	The maximum time allotted to the process that clears the operating system's firewall rules. If the process does not signal its completion within this time, the Watchdog server considers the process to be frozen.	Default value: 10 seconds.
`TimeoutAfterClean`	The maximum time allotted to the process that clears the operating system's firewall rules to finish after the Watchdog server has sent the SIGTERM signal to the cleaning process.	Default value: 10 seconds.
By default, the **[Environment]** section is absent from the configuration file.		
`ExperimentalContainerdSupport`	Enabling support for the containerd environment when running the Container Monitoring component. By default, this section is absent from the configuration file. If you want to use the containerd environment when the Container Monitoring component is running, you need to manually add the `[Environment]` section to the configuration file and inside it, the `ExperimentalContainerdSupport` setting. This setting is not applicable to devices with an Elbrus CPU.	`true/yes` – enable support for the containerd environment in the operation of the Container Monitoring component. `false/no` – do not enable support for the containerd environment in the operation of the Container Monitoring component.
`ReduceSWMemoryConsumption`	Limiting the memory consumption by the Behavior Detection component for processing the event queue. Setting a memory limit negatively affects threat detection, including the quality of telemetry transmitted as part of integration with Detection and Response solutions. We recommend setting a limit only on highly loaded systems and after contacting Technical Support to get specific instructions, if there are no other options for solving the problem of high memory consumption.	1 – limit the memory usage by the Behavior Detection component for processing the event queue. 0 (default) – do not limit memory usage. The application must be restarted after this setting is changed.

Default settings for command line tasks

This section contains the default options for all predefined tasks that are provided for managing Kaspersky Endpoint Security via the command line.

The `Rollback` and `License` tasks have no settings.

Default settings for the File_Threat_Protection task (ID:1)

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

SkipDatabaseJournals=No

TimeLimit=60

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanByAccessType=SmartCheck

[ScanScope.item_0000]

AreaDesc=All objects
```

UseScanArea=Yes

Path=/

AreaMask.item_0000=*

Default settings for the Scan_My_Computer task (ID:2)

ScanFiles=Yes

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

```
[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Default settings for the Scan_File task (ID:3)

```
ScanFiles=Yes

ScanBootSectors=No

ScanComputerMemory=No

ScanStartupObjects=No

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

UseGlobalExclusions=Yes
```

```
UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Default settings for the Critical_Areas_Scan task (ID:4)

```
ScanFiles=No

ScanBootSectors=Yes

ScanComputerMemory=Yes

ScanStartupObjects=Yes

ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

QueueScanTasks=No

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended
```

```
UseIChecker=Yes

UseGlobalExclusions=Yes

UseOASExclusions=Yes

DeviceNameMasks.item_0000=/**

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/

AreaMask.item_0000=*
```

Default settings for the Update task (ID:6)

```
ConnectionTimeout=10

ApplicationUpdateMode=DownloadOnly

[Sources.item_0000]

Enabled=Yes

SourceType=KLServers

URL=
```

Default settings for the System_Integrity_Monitoring task (ID:11)

```
UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=Kaspersky internal objects

UseScanArea=Yes

Path=/opt/kaspersky/kesl/

AreaMask.item_0000=*
```

Default settings for the Firewall_Management task (ID:12)

```
DefaultIncomingAction=Allow
```

```
DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Default settings for the Anti_Cryptor task (ID:13)

```
ActionOnDetect=Block

BlockTime=30

UseExcludeMasks=No

[ScanScope.item_0000]

AreaDesc=All shared directories

UseScanArea=Yes

Path=AllShared

AreaMask.item_0000=*
```

Default settings for the Web_Threat_Protection task (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Default settings for the Device_Control task (ID:15)

```
OperationMode=Block

AllowToRequestTemporaryAccess=No
```

```
[DeviceClass]

HardDrive=DependsOnBus

RemovableDrive=DependsOnBus

Printer=DependsOnBus

FloppyDrive=DependsOnBus

OpticalDrive=DependsOnBus

Modem=DependsOnBus

TapeDrive=DependsOnBus

MultifuncDevice=DependsOnBus

SmartCardReader=DependsOnBus

PortableDevice=DependsOnBus

WiFiAdapter=DependsOnBus

NetworkAdapter=DependsOnBus

BluetoothDevice=DependsOnBus

ImagingDevice=DependsOnBus

SerialPortDevice=DependsOnBus

ParallelPortDevice=DependsOnBus

InputDevice=DependsOnBus

SoundAdapter=DependsOnBus

[DeviceBus]

USB=Allow

FireWire=Allow

[Schedules.item_0000]

ScheduleName=Default

DaysHours=All

[HardDrivePrincipals.item_0000]

Principal=\Everyone
```

```
[HardDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[RemovableDrivePrincipals.item_0000]

Principal=\Everyone

[RemovableDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[FloppyDrivePrincipals.item_0000]

Principal=\Everyone

[FloppyDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow

[OpticalDrivePrincipals.item_0000]

Principal=\Everyone

[OpticalDrivePrincipals.item_0000.AccessRules.item_0000]

UseRule=Yes

ScheduleName=Default

Access=Allow
```

Default settings for the Removable_Drives_Scan task (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Default settings for the Network_Threat_Protection task (ID:17)

```
ActionOnDetect=Block

BlockAttackingHosts=Yes

BlockDurationMinutes=60

UseExcludeIPs=No
```

Default settings for Container_Scan (ID:18) and Custom_Container_Scan (ID:19) tasks

```
ScanArchived=Yes

ScanSfxArchived=Yes

ScanMailBases=No

ScanPlainMail=No

TimeLimit=0

SizeLimit=0

ActionOnThreat=DisinfectDeleteIfNotPossible

UseExcludeMasks=No

UseExcludeThreats=No

ReportCleanObjects=No

ReportPackedObjects=No

ReportUnprocessedObjects=No

UseAnalyzer=Yes

HeuristicLevel=Recommended

UseIChecker=Yes

ScanContainers=Yes

ContainerNameMask=*

ScanImages=Yes

ImageNameMask=*
```

```
DeepScan=No

ContainerScanAction=StopContainerIfFailed

ImageAction=Skip

UseGlobalExclusions=Yes

QueueScanTasks=No
```

You can also use the option in this configuration file for the Custom Container Scan task.

Default settings for the Behavior_Detection task (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block

UseAEP=No

AEPMode=Block

UseTelemetryMonopolyMode=Yes

TelemetrySource=Default
```

Default settings for the Application_Control task (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Default settings for the Inventory_Scan task (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

GoldenImageAction=DoNothing

[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes
```

```
Path=/usr/bin

AreaMask.item_0000=*
```

Default settings for KATAEDR task (ID:24)

```
Mode=EDRKATA

UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=127.0.0.1

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

[TelemetrySettings]

UseClientPinnedCertificate=No

ConnectionTimeout=10

RequestTimeout=10

OnlyTaggedEvents=No

[TelemetrySettings.Endpoints.item_#]

Address=

Port=443

[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
```

```
UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Default settings for the Web_Control task (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

Default settings for the Standalone_Sandbox task (ID:29)

```
ConnectionTimeout=10

RequestTimeout=10

UseClientCertificate=No

SendingMode=AutoOnly

QuarantineFile=Yes

ScanCriticalAreas=Yes

CreateIocScanTask=Yes

QuarantineFileOnIocDetected=Yes

ScanCriticalAreasOnIocDetected=Yes

Drives=Critical

ScheduleMode=Manually

[Servers.item_0000]

Address=127.0.0.1

Port=443

[SandboxTransferSettings]

SandboxQueue=1024
```

Default settings for KATANDR task (ID:31)

```
UseClientPinnedCertificate=No
```

```
SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

[Endpoints.item_0000]

Address=127.0.0.1

Port=8081

[EventTransferSettings]

MaximumDataTransferTime=30

MaximumNumberOfEventsInPackage=1024

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15

PingPeriod=450
```

Default settings for the KUMA task (ID:33)

```
UseClientCertificate=No

UseTls=No

ConnectionTimeout=5

[Servers.item_0000]

Address=127.0.0.1

Port=443

Protocol=TCP

[SiemTransferSettings]

EventTransferTimeMax=30
```

Default settings of the Mail Threat Protection task (ID: 35)

```
CheckIncomingMessagesOnly=No

ActionOnThreat=DisinfectDeleteIfNotPossible
```

```
ScanFileArchive=Yes

ScanFileOffice=Yes

UseTimeLimit=No

TimeLimit=8

UseSizeLimit=No

SizeLimit=5

ExtensionFilter=Rename

UseAnalyzer=Yes

AnalyzerLevel=Medium

[ExtensionMasks.item_0000]

UseExtensionMask=Yes

ExtensionMask=*.txt

[ExtensionMasks.item_0001]

UseExtensionMask=Yes

ExtensionMask=*.run

[ExtensionMasks.item_0002]

UseExtensionMask=Yes

ExtensionMask=*.exe

[ExtensionMasks.item_0003]

UseExtensionMask=Yes

ExtensionMask=*.js

[ExtensionMasks.item_0004]

UseExtensionMask=Yes

ExtensionMask=*.jse

[ExtensionMasks.item_0005]

UseExtensionMask=Yes

ExtensionMask=*.msi
```

```
[ExtensionMasks.item_0006]

UseExtensionMask=Yes

ExtensionMask=*.scr

[ExtensionMasks.item_0007]

UseExtensionMask=Yes

ExtensionMask=*.vbe

[ExtensionMasks.item_0008]

UseExtensionMask=Yes

ExtensionMask=*.vbs

[ExtensionMasks.item_0009]

UseExtensionMask=Yes

ExtensionMask=*.sh
```

Default settings of the BadUSB Attack Prevention task (ID: 37)

```
MaxAuthAttempts=5

TimeoutAfterAttempts=5

ProhibitOnScreenKeyboard=No

ProhibitBarcodeScanner=Yes
```

Default settings for KATANDR task (ID:31)

```
ConnectionTimeout=10

RequestTimeout=10

SynchronizationPeriod=5

UseTunnel=No

TunnelAddress=127.0.0.1

TunnelPort=443

[Endpoints.item_0000]

Address=127.0.0.1
```

```
Port=443
EnableTelemetry=Yes
[TelemetrySettings]

ConnectionTimeout=10
RequestTimeout=10
OnlyTaggedEvents=No
UseTunnel=No
TunnelAddress=127.0.0.1
TunnelPort=443
[TelemetrySettings.Endpoints.item_0000]

Address=127.0.0.1
Port=443
[TelemetrySettings.EventTransferSettings]

MaximumDataTransferTime=30
UseRequestCountLimits=Yes
MaximumNumberOfEventsInHour=3000
EventLimitExceededPercentage=15
MaximumNumberOfEventsInPackage=1024
```

Appendix 2. Configuring interaction with Kaspersky Anti-Virus for Linux Mail Server

To configure joint operation of Kaspersky Endpoint Security and Kaspersky Anti-Virus for Linux Mail Server:

1. Save the File Threat Protection task settings in the configuration file using the following command:

   ```
   kesl-control --get-settings 1 --file <full path to file>
   ```

2. Open the created configuration file for editing.

3. Add the following section to the created file:

   ```
   [ExcludedFromScanScope.item_<item number>]
   Path=/var/opt/kaspersky/klms
   ```

4. Repeat the section specified above for all mail agents integrated with Kaspersky Anti-Virus for Linux Mail Server.

5. To exclude the temporary directory of filters and services of Kaspersky Anti-Virus for Linux Mail Server from scanning, add the following section to the created file:

   ```
   [ExcludedFromScanScope.item_<item number>]
   Path=/tmp/klmstmp
   ```

6. Save the changes in the configuration file.

7. Import settings from the configuration file to the File Threat Protection task by using the following command:

```
kesl-control --set-settings 1 --file <full path to file>
```

Appendix 3. Settings for interaction with external services

Kaspersky Endpoint Security uses the following network settings and encryption settings for interaction with external services.

Settings for interaction with external services

Network address of the service and protocol	Description
`activation-v2.kaspersky.com/activationservice/activationservice.svc` Protocol: HTTPS Port: 443	Application activation.

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
Protocol: HTTPS
Port: 443
	Updating application databases and modules.

Network address of the service and protocol	Description

`p00.upd.kaspersky.com`
`p01.upd.kaspersky.com`
`p02.upd.kaspersky.com`
`p03.upd.kaspersky.com`
`p04.upd.kaspersky.com`
`p05.upd.kaspersky.com`
`p06.upd.kaspersky.com`
`p07.upd.kaspersky.com`
`p08.upd.kaspersky.com`
`p09.upd.kaspersky.com`
`p10.upd.kaspersky.com`
`p11.upd.kaspersky.com`
`p12.upd.kaspersky.com`
`p13.upd.kaspersky.com`
`p14.upd.kaspersky.com`
`p15.upd.kaspersky.com`
`p16.upd.kaspersky.com`
`p17.upd.kaspersky.com`
`p18.upd.kaspersky.com`
`p19.upd.kaspersky.com`
`downloads.kaspersky-labs.com`
Protocol: `HTTP`
Port: `80`
	Updating application databases and modules.

`downloads.upd.kaspersky.com` Protocol: `HTTPS` Port: `443`	• Updating application databases and modules. • Checking access to Kaspersky servers. If there are errors accessing servers through the system DNS, the application uses a public DNS. This is needed for updating application databases and maintaining device security. The application will use the following public DNSes in this order: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168). The application's requests may contain domain addresses and the user's external IP address, since the application establishes a TCP/UDP connection with the DNS server. This information is necessary, for example, to check the certificate of a web resource when interacting via HTTPS. If the application is using a public DNS server, data processing rules are governed by the Privacy Policy of the corresponding service.
`ds.kaspersky.com` Protocol: `HTTPS` Port: `443`	Using Kaspersky Security Network.

Network address of the service and protocol	Description

`ksn-a-stat-geo.kaspersky-labs.com`
`ksn-file-geo.kaspersky-labs.com`
`ksn-verdict-geo.kaspersky-labs.com`
`ksn-url-geo.kaspersky-labs.com`
`ksn-a-p2p-geo.kaspersky-labs.com`
`ksn-cinfo-geo.kaspersky-labs.com`
Protocol: `KSN`
Port: `443`, `1443`
	Using Kaspersky Security Network.

`click.kaspersky.com` Protocol: `HTTPS` Port: `443`	Following links from the user interface.

`crl.kaspersky.com`
`ocsp.kaspersky.com`
Protocol: `HTTP`
Port: `80`
	Public Key Infrastructure (PKI).
	These servers (crl.kaspersky.com) are part of the public key infrastructure (PKI) and are required for verifying the validity status of Kaspersky digital signature certificates. The CRL server provides a list of revoked certificates. The OCSP service allows querying the status of a specific certificate in real time. These components maintain the security of interaction with digital certificates and provide protection against possible attacks.

Appendix 4. File extensions for quick removable drives scan

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

msg – Microsoft Mail email message

plg – email message

mbx – saved Microsoft Office Outlook email message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file;

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates, xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsm for Microsoft Office Excel 2007 templates with macro support, and xlam for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

Appendix 5. Variables in message templates

The Device Control and Web Control components let you configure templates of messages that Kaspersky Endpoint Security displays to a user trying to gain access to a blocked device, application, or resource, or attempting to perform a potentially dangerous action.

Special variables are provided for managing the message templates (for example, %USER_NAME%). Variables allow a single message template to be used for different computers. When generating a message, Kaspersky Endpoint Security retrieves the value of the variable from the operating system settings and inserts it into the message matching the specific computer, user, and event.

Variables in Device Control message templates

You can use the following variables in user message templates or administrator message templates:

- **User** – %USER_NAME%.

  Name of the current user account on the computer on which the message was generated, in the <device name>\<user alias> format (for example, DESKTOP-123\John.Smith).

- **Computer name** – %COMPUTER_NAME%.

  Name of the computer on which a device was blocked.

- **Rule name** – %RULE%.

  Name of the rule that blocked the device.

- **Rule triggering date** – %DATE%.

  Date when the device was blocked in the DD.MM.YYYY format.

- **Rule triggering time** – %TIME%.

  Time when the device was blocked in the HH:MM format.

- **Device name** – %DEVICE_NAME%.

  Name of the blocked device.

- **Device type** – %DEVICE_TYPE%.

  Type of the blocked device (for example, printers, removable drives, CD/DVD drives).

- **Device model** – %DEVICE_VIDPID%.

  Model of the blocked device (for example, VID_1234&PID_5678).

- **Device ID** – %DEVICE_ID%.

  ID of the blocked device (for example, SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000).

- **Device operations** – %OPERATION%.

  Type of the forbidden operation with the device.

Variables in Web Control message templates

You can use the following variables in user message templates or administrator message templates:

- **User** – %USER_NAME%.

  Name of the current user account on the computer on which the message was generated, in the <device name>\<user alias> format (for example, DESKTOP-123\John.Smith).

- **Web resource address** – %CANONIC_REQUEST_URL%.

  Address of the blocked web resource.

- **Rule name** – `%RULE%`.

  Name of the rule that blocked the web resource.

- **Email for sending a message** – `%COMPLAIN_EMAIL%`.

  Email address for feedback about web resource blocks. Clicking the email address opens a window in which the user can write a message to the administrator.

- **Name of content category** – `%CONTENT_CATEGORY_LIST%`.

  Website category to which the blocked resource belongs (for example, *Payment systems*).

- **Name of data type category** – `%TYPE_CATEGORY_LIST%`.

  Category of data type on the blocked web resource (for example, *Graphic files*).

- **Link to requested web resource** – `%CONTINUE_PAGE%`.

  Link to the requested web page (for example, `http://www.example.com/pagename.html`).

- **Link to website** – `%CONTINUE_SITE%`.

  Link to the website that contains the requested web page (for example, `http://www.example.com/`).

- **Link for access to domains** – `%CONTINUE_DOMAIN%`.

  Link that can be clicked to gain access to all existing web pages of the domain name. For example, if the address of the blocked web page is `http://www.example.com`, the `%CONTINUE_DOMAIN%` variable is replaces with the `http://*.example.com` link. Clicking this link allows access to all web addresses of the base domain name `http://www.example.com/` including subdomains, for example, `http://start.example.com/*` or `http://domain.domain.example.com/*`, where the `*` character stands for any sequence of characters (including an empty string).

Appendix 6. Application events

Information about the operation of each Kaspersky Endpoint Security component, data encryption events, the completion of each malware scan task, update task and integrity check task, and the overall operation of the application is recorded in the Kaspersky Security Center event log and operating system event log (syslog).

Critical

System integrity violation

Status	!
Component	System Integrity Monitoring
Linux event ID	0
Kaspersky Security Center event ID	`GNRL_EV_FIM_ALARM`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Application startup denied

Status	!
Component	Application Control
Linux event ID	122
Kaspersky Security Center event ID	`GNRL_EV_APPLICATION_LAUNCH_DENIED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Malicious object detected (local databases)

Status	!
Component	File Threat Protection Mail Threat Protection Behavior Detection Exploit Prevention Sandbox
Linux event ID	6
Kaspersky Security Center event ID	`GNRL_EV_VIRUS_FOUND`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

System Integrity Monitoring event limit exceeded

Status	!
Component	System Integrity Monitoring
Linux event ID	70
Kaspersky Security Center event ID	`GNRL_EV_FIM_ALARM_OVERFLOW`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Operation with the device prohibited

Status	!
Component	Device Control
Linux event ID	94
Kaspersky Security Center event ID	`GNRL_EV_DEVCTRL_DEV_PLUG_DENIED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Network attack detected

Status	!
Component	Network Threat Protection
Linux event ID	102
Kaspersky Security Center event ID	`GNRL_EV_ATTACK_DETECTED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Access denied (local databases)

Status	⊘
Component	Web Control
Linux event ID	190
Kaspersky Security Center event ID	`GNRL_EV_WEB_URL_BLOCKED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Warning

Disinfection impossible

Status	⚠
Component	File Threat Protection Mail Threat Protection
Linux event ID	10
Kaspersky Security Center event ID	`GNRL_EV_OBJECT_NOTCURED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Warning about undesirable content (local data bases)

Status	⚠
Component	Web Control
Linux event ID	192
Kaspersky Security Center event ID	`GNRL_EV_WEB_URL_WARNING`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Message to the administrator regarding the blocking of access to a web page

Status	⚠
Component	Web Control
Linux event ID	196
Kaspersky Security Center event ID	`GNRL_EV_WC_USER_REQUEST`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Informational message

Object disinfected

Status	ⓘ
Component	File Threat Protection Mail Threat Protection
Linux event ID	9
Kaspersky Security Center event ID	`GNRL_EV_OBJECT_CURED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Object deleted

Status	ⓘ
Component	File Threat Protection Mail Threat Protection
Linux event ID	8
Kaspersky Security Center event ID	`GNRL_EV_OBJECT_DELETED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Application startup allowed

Status	ⓘ
Component	Application Control
Linux event ID	120
Kaspersky Security Center event ID	`GNRL_EV_APPLICATION_LAUNCHED`
Log (syslog) (default)	–
Kaspersky Security Center event log	not configured

Application startup allowed in test mode

Status	ⓘ
Component	Application Control
Linux event ID	121
Kaspersky Security Center event ID	`GNRL_EV_APP_LAUNCH_TESTED_ALLOW`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Application startup denied in test mode

Status	ⓘ
Component	Application Control
Linux event ID	123
Kaspersky Security Center event ID	GNRL_EV_APP_LAUNCH_TESTED_DENIED
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Device connected

Status	ⓘ
Component	Device Control
Linux event ID	90
Kaspersky Security Center event ID	`GNRL_EV_DEVCTRL_DEV_PLUGGED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Device disconnected

Status	ⓘ
Component	Device Control
Linux event ID	91
Kaspersky Security Center event ID	`GNRL_EV_DEVCTRL_DEV_UNPLUGGED`
Log (syslog) (default)	–
Kaspersky Security Center event log (default)	✓

Appendix 7. Return codes

Return codes of the initial configuration wizard

0 – Installation completed successfully.

Critical errors

1 – Unknown error (all other critical errors, except those listed below, for example: system errors, insufficient memory, file opening error, and others).

2 – The initial configuration file contains invalid parameters.

3 – Failed to install or update the application.

4 – Unable to remove the application.

5 – Unable to start the application. Potential reason: access rights are configured incorrectly. Check that only the root account has the right to write to the following directories: /, /opt, /opt/kaspersky, /var, /var/opt, /var/opt/kaspersky, /usr, and /usr/lib64.

6 – The necessary actions have not been performed prior to installation.

7 – Failed to update the application. Installing an earlier version of the application is not supported.

8 – Failed to remove users from privileged groups.

9 – Failed to create a unique MachineID for the application installation.

10 – Failed to start or restart the application.

11 – The terms and conditions of the End User License Agreement (EULA) and Privacy Policy have not been accepted.

12 – The application cannot be used in Light Agent mode and in EDR Agent mode at the same time.

13 – The astra-digsig-oldkeys package for the closed software environment mode in Astra Linux was not found.

14 – Initial configuration has already been started.

15 – The Light Agent for Linux component, installed as part of the Kaspersky Security for Virtualization 5.2 Light Agent solution, must be removed.

16 – Kaspersky Security Center Network Agent must be installed.

17 – Failed to start the Initial Configuration Wizard due to an application process already running.

18 – fanotify is not supported. Failed to compile a kernel module for File Threat Protection.

19 – Administrator rights are required for installation.

20 – The application service has not been started.

21 – The application update has been rolled back.

22 – Integration of the application in EDR agent mode or Light Agent mode with Kaspersky Endpoint Detection and Response Expert (cloud) is not supported.

Warnings

71 – Multiple warnings during installation. See the installation log for more details.

72 – Failed to update application databases.

75 – Operating system restart is required.

76 – Failed to apply the KSN settings or the terms and conditions of the KSN Statement were not accepted.

77 – Failed to start an updatable kernel module.

79 – Failed to install or update the graphical interface package of the application.

80 – Failed to download application databases.

81 – Activation of the application ended with an error due to network problems.

82 – The application is managed by a policy.

83 – Application GUI was not started.

84 – Failed to assign the administrator role. The specified user was not found.

85 – The application package could only be installed or updated in error-ignoring mode of the package manager.

86 – Failed to remove the graphical interface package of the application.

87 – The application package could only be removed in error-ignoring mode of the package manager.

88 – Failed to assign the administrator role to the user.

89 – Invalid license key.

90 – Failed to set a schedule for the update task.

Return codes of the kesl-control command-line utility

0 – Command/task completed successfully.

1 – General error in command syntax.

2 – Error in passed application settings.

64 – Kaspersky Endpoint Security is not running.

66 – Application databases are not loaded (used only by the `kesl-control --app-info` command).

67 – Activation of the application ended with an error due to network problems.

68 – The command cannot be executed because the application is managed by a policy.

69 – The application is located in the Amazon Paid Ami infrastructure.

70 – An attempt to start a task that is already running, delete a running task, change the settings of a running task, stop a stopped task, pause a suspended task, or resume a running task.

71 – Kaspersky Security Network Statement has not been accepted.

72 – Threats were detected during execution of the Custom Scan or Custom Container Scan task.

73 – Attempt to set Application Control task settings that affect the operation of the application without confirming them using the `--accept` option.

74 – Kaspersky Endpoint Security must be restarted after an update.

75 – The device must be restarted.

76 – Connection prohibited, as only users with root rights should have write access to the specified path.

77 – The specified license key is already in use on the device.

78 – The command/task cannot be run because the application is being used in Light Agent mode.

79 – The command cannot be run because the application is being used in standard mode.

80 – The update download operation failed due to network problems.

81 – The component is not supported in the version of the operating system that is installed on the device.

128 – Unknown error.

65 – all other errors.

Appendix 8. Preparing an archive with application databases

When manually creating a Kaspersky Endpoint Security installation package, you can add previously downloaded application databases to it. If you are using an installation package with integrated databases, the application is installed together with the databases; in this case, you do not need to update the databases immediately after installation.

Adding application databases to the installation package makes the package larger.

You will need a separate set of application databases for each combination of architecture and bitness of the operating system on your protected devices. You can add an archive containing one or more sets of application databases in the installation package. To prepare each set of application databases, you need an instance of the Kaspersky Endpoint Security application already installed on a device with an operating system of matching architecture and bitness.

To prepare an archive with databases:

1. Install and perform the initial configuration of Kaspersky Endpoint Security on the device using Kaspersky Security Center or using the command line.

2. Update application databases on the device. You can update the databases during the initial configuration of the application or after installation by running an *Update* task on the command line or an *Update* task in the Kaspersky Security Center.

3. Create a directory for the databases, depending on the architecture and bitness of the operating system on the protected device:

   - x86_64 if the application is installed on a 64-bit operating system

   - i386 if the application is installed on a 32-bit operating system

   - arm64 if the application is installed on a 64-bit operating system for the Arm architecture

   - e2k if the application is installed on a 64-bit operating system for the Elbrus architecture

4. Copy the contents of the /var/opt/kaspersky/kesl/private/updates directory to the created database directory.

5. Add the created database directory to the kesl-bases.tgz archive.

   If you want to create an installation package for installation on multiple operating systems with different architectures and bitnesses, you need to prepare several directories with databases and add them all to the kesl-bases.tgz archive.

By default, the database update task is started after the installation of the Kaspersky Endpoint Security application. If you are installing an application from an installation package with integrated databases, disable the database update task after installing the application. You can configure this setting in the properties of the created installation package or in the autoinstall.ini configuration file (`UPDATE_EXECUTE=No`).

Appendix 9. Requirements for IOC files

When creating IOC Scan tasks, consider the following IOC file requirements and limitations:

- The application supports IOC files with the .IOC or .XML extension in OpenIOC format versions 1.0 and 1.1, an open standard for describing indicators of compromise.
- Semantic errors and unsupported IOC terms and tags in IOC files do not cause the task to fail. For such sections of IOC files, the application registers the absence of a match.
- IDs of all IOC files used in an IOC Scan task must be unique. If there are IOC files with the same identifier, it might affect the task execution results.
- We recommend creating an IOC file for each threat. This makes the results of the *IOC Scan* task easier to read.

The file that can be downloaded by clicking the link below contains a table with the full list of IOC terms of the OpenIOC standard.

DOWNLOAD THE IOC TERMS.XLSX FILE

Special considerations and limitations of the way the application supports the OpenIOC standard are listed in the table below.

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 attributes of conditions	OpenIOC 1.1: • `preserve-case` • `negate`
Supported operators	`AND` `OR`
Supported data types	`"date"`: date (applicable conditions: `is`, `greater-than`, `less-than`) `"int"`: integer (applicable conditions: `is`, `greater-than`, `less-than`) `"string"`: string (applicable conditions: `is`, `contains`, `matches`, `starts-with`, `ends-with`) `"duration"`: duration in seconds (applicable terms: `is`, `greater-than`, `less-than`)

Special considerations for interpreting data types	The `"boolean string"`, `"restricted string"`, `"md5"`, `"IP"`, `"sha256"`, `"base64Binary"` data types are interpreted as strings.
	The application supports the interpretation of the `Content` parameter for `int` and `date` data types specified as intervals:
	• 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 `greater-than` and `less-than` conditions
	  • Using the `TO` operator in the `Content` field
	The application supports the interpretation of the `date` and `duration` data types if the indicators are specified in the `ISO 8601, Zulu time zone, UTC` format.

Legal notice

Data provision

This section describes the information that Kaspersky Endpoint Security may store on the device and automatically send to Kaspersky during its operation.

Kaspersky protects any information thus received in accordance with law and the applicable rules of Kaspersky. Data is transmitted over encrypted channels.

For detailed information about the processing, storage, and destruction of information obtained during the use of the application and transmitted to Kaspersky, please read the End User License Agreement, the Kaspersky Security Network Statement, and the Privacy Policy on the Kaspersky website. The license.<language ID> and ksn_license.<language ID> files containing the End User License Agreement and Kaspersky Security Network Statement are included in the application distribution package.

Data provided when using an activation code

If Kaspersky Endpoint Security is used in standard mode or in EDR Agent mode and is activated using an activation code, in order to verify if the application is being used legally and to obtain statistical information on the distribution and use of the application, you agree to automatically provide the following information to Kaspersky:

- type, version, and localization of the installed application;
- versions of installed application updates;
- device ID and application installation ID on the device;
- activation code that was used to activate the application;
- ID of the current license;
- application license key creation date and time;
- date and time on the user's device;
- application license term expiration date and time;
- type, version, and bit size of the operating system.

Data provided when downloading updates from Kaspersky update servers

If Kaspersky Endpoint Security is being used in standard mode or EDR Agent mode, and you use Kaspersky update servers to download updates, to improve the efficiency of the update procedure and to provide statistical information about the distribution and usage of the application, you agree to automatically provide the following information to Kaspersky:

- application ID derived from the license;
- full version of the application;
- application license ID;
- type of application license used;
- application installation ID (PCID);
- ID of the application update start;
- web address being processed.

Data transferred when using the application in Light Agent mode

If Kaspersky Endpoint Security is used in Light Agent mode as part of Kaspersky Security for Virtualization Light Agent, the application saves the following information, which may contain personal and confidential data, and sends it to other solution components during operation of the application.

- For activation, Kaspersky Endpoint Security sends the following data to the Protection Server: the validity period of the license key status confirmation, the BIOS ID of the protected virtual machine, and information about the license that the Light Agent needs to work.
- To update the Light Agent databases, Kaspersky Endpoint Security sends the following data to the Protection Server: software identifier obtained from the license; full version of the software; software license identifier; software installation identifier (PCID); processed web address; type of the license; identifier of the update start.
- To provide protection, Kaspersky Endpoint Security sends the Protection Server the information that is necessary for scanning objects while scan tasks are running. The transmitted information may include the names of files and paths to them in the file system, the checksums of files, web addresses, and the scanned objects or their fragments.
- In an infrastructure managed by a VMware vCenter Server and VMware NSX Manager, Kaspersky Endpoint Security may send to the Integration Server information about security tags that are assigned to a protected virtual machine upon detection of viruses, malware, or activity that is typical of network attacks. The IDs of protected virtual machines are also sent.
- To get information that is used when selecting an SVM for connection, Kaspersky Endpoint Security sends the identifier of the protected virtual machine to the Integration Server and Protection Server.

- When using the Kaspersky Security for Virtualization Light Agent solution in multitenancy mode, the information necessary for generating tenant protection reports may be sent to SVMs from the Kaspersky Endpoint Security Protection Server. The following data may be sent: identifier of the protected virtual machine; type and version of the guest operating system installed on the protected virtual machine; time intervals when Kaspersky Endpoint Security was connected to SVMs.

- To obtain statistics, Kaspersky Endpoint Security sends the following information to the Protection Server: information about the OS version of the protected virtual machine; localization of Kaspersky Endpoint Security; names of active Kaspersky Endpoint Security components; identifier (BIOS ID) of the protected virtual machine.

The specified information is transmitted over encrypted data channels (except for the information necessary for scanning objects, and the information that is used when selecting SVMs). The connection between Kaspersky Endpoint Security and the Protection Servers is not encrypted by default. You can enable encryption of the data channel between the Light Agents and the Protection Servers in the Kaspersky Endpoint Security settings.

Data sent to Kaspersky Security Center

During operation, Kaspersky Endpoint Security saves and submits to Kaspersky Security Center the following information, which may contain personal and confidential data:

- Information about the databases used by the application:
  - List of the database categories required by the application
  - Date and time when the databases were released and loaded into the application
  - Date when the downloaded application database updates were released
  - Time of the last application database update
  - Number of records in the currently used application databases
- Application license information:
  - License serial number and type
  - License validity period in days
  - Number of devices covered by the license
  - Start and end dates of license term
  - License key status
  - Date and time of the last successful synchronization with activation servers if the application was activated using an activation code
  - Identifier of the application for which the license is intended
  - Functionality available under the license
  - Name of the organization for which the license is provided

- Additional information if the application is used under subscription (subscription flag, subscription expiration date and the number of days available for renewing the subscription, subscription provider web address, current subscription status and the reason for this status), date and time when the application was activated on the device
- Expiration date and time of the application license on the device

- Information about the application updates:
  - List of updates to be installed or removed
  - Update release date and the sign of the *Critical* status
  - Name, version, and short description of the update
  - Link to the detailed description of the update
  - Identifier and text of the End User License Agreement and the Privacy Policy for the application updates
  - Identifier and text of Kaspersky Security Network Statement for the application updates
  - Indicator showing if the update can be removed
  - Versions of the application policy and management plug-in
  - Web address for downloading the application management plug-in
  - Names, version, and installation dates of the installed application updates
  - Error code and description if the update installation or removal completed with an error
  - Sign and reason for the device or application restart necessity because of the application update
- User agreement or disagreement with the terms and conditions of Kaspersky Security Network Statement, End User License Agreement and Privacy Policy
- List of tags assigned to the device
- List of device statuses and reasons they are assigned.
- The overall status of the application and the status of all its components; information about policy compliance, real-time protection status of the device, application stability status, information about the application stopping.
- Date and time of the last device scan; number of scanned objects; number of detected malicious objects; number of blocked, deleted and disinfected objects; number of objects that cannot be disinfected; number of scan errors; number of detected network attacks
- Data on the currently applied values of the application settings
- Current status and execution results of group tasks and local tasks, and settings of the tasks.
- Information about external devices connected to the client device (ID, name, type, manufacturer, description, serial number, VID/PID)

- Information about backup copies of files in the Backup storage (name, path, size and type of the object, description of the object, name of the detected threat, version of the application database which is used to detect the threat, date and time when the object was moved to the Backup storage), actions on the objects in the Backup storage (removed, restored), and the files by administrator request.

- Information about the operation of each application component and about the execution of each task represented as events:

  - Date and time of event

  - Name and type of event

  - Event severity level

  - Name of the task or the application component running when the event occurred

  - Information about the application that triggered the event: application name, path to the file on the disk, process identifier, setting values (if the application launch or settings modification event is triggered)

  - User ID

  - Name of the initiator (task scheduler, application, Kaspersky Security Center, or a user) whose actions triggered the event

  - Name and identifier of the user who initiated access to the file

  - Object or action processing result (description, type, name, threat level and accuracy, file name and type of operation on the device, application decision on the operation)

  - Information about the object (object name and type, path to the object on the disk, object version, size, information about the performed action, event trigger description, description of the reason for not processing and skipping the object)

  - Device information (manufacturer name, device name, path, device type, bus type, identifier, VID/PID, system device flag, name of the device access rule schedule)

  - Information about blocking and unblocking the device; information about blocked connections (name, description, device name, protocol, remote address and port, local address and port, packet rules, actions)

  - Information about requested web address

  - Information about detected objects

  - Type, method, and ID of the detection

  - Information about the performed action

  - Information about the application databases (date when the downloaded database updates are released, information on the database usage, database usage errors, information on canceling the installed database updates)

  - Information about encryption detection (ransomware name; name of the device where encryption was detected; information about blocking and unblocking the device)

  - Application settings and network settings

    - Information about the triggered Application Control rule (name and type) and the result of applying the rule
    - Information about containers and container images (names of containers or container images, paths to containers or container images, repository URL)
    - Information about active and blocked connections (name, description, and type)
    - Information about blocking and unblocking access to untrusted devices
    - Information about the use of KSN (KSN connection status, KSN infrastructure, identifier of the KSN Statement in extended mode, acceptance of the KSN Statement in extended mode, identifier of the KSN Statement, acceptance of the KSN Statement)
    - Information about certificates (domain name, subject name, issuer name, expiration date, certificate status, certificate type, date certificate was added, issue date, serial number, SHA256 thumbprint)
    - Information about external systems that are part of corporate software solutions (integration server address)
    - Information about enabling and disabling network isolation for the device
    - Information about working in Light Agent mode: name of the virtual machine template, address of the Integration Server
    - Name of the device for which network isolation is enabled or disabled
    - Scan task statistics: number of scanned objects; number of threats found; number of infected objects; number of probably infected objects; number of disinfected objects; number of objects added to Backup; number of deleted objects; number of not disinfected objects; number of scan errors; number of password-protected objects; number of skipped objects; number of scanned containers and images
    - Information about the version of the EDR Optimum component used in the application
    - Information about threat development chains: name of the online list of threat development chains, ID of the threat development chain
- Information about operation of the system integrity scan task (name, type, path) and information about the system baseline
- Information about network activity, packet rules, and network attacks
- User role information:
    - Name and identifier of the user who initiated changing the user role
    - User role
    - Name of the user who has been assigned or revoked the role

- Information about executable files of applications detected on the client device (name, path, type, and hash of the file; list of categories to which the application belongs; KL category to which the application belongs; trust group to which the application belongs; time of the first file launch; name and version of the application; name of the application vendor; information about the certificate used to sign the application: serial number, thumbprint, issuer, subject, release date, expiration date, and public key).

- Information about the online list of threat development chains: threat development chain ID; creation timestamp of the threat development chain; format of the threat development chain (text or archive); body size of the threat development chain in bytes.

Data provided when following links in the application interface

When clicking the links in Kaspersky Endpoint Security interface, you agree to automatically provide the following information to Kaspersky:

- full version of the application;

- application locale;

- application ID (PID);

- link name.

Data provided when using Kaspersky Security Network

The set of data that Kaspersky Security Network provides to Kaspersky depends on the Kaspersky Security Network mode.

The ksn_license.<language ID> file with the text of the Kaspersky Security Network Statement is included in the application distribution kit.

Data provision in Basic KSN mode

If you are using Kaspersky Security Network in Basic KSN mode (the **Use of Kaspersky Security Network (KSN)** toggle switch is enabled and the **Use Extended KSN mode** check box is cleared in the Web Console, the **Basic KSN mode** option is selected in the Administration Console), by accepting the terms and conditions of the Kaspersky Security Network Statement, you agree to automatically provide the following information to Kaspersky.

Data provision in Extended KSN mode

If you are using Kaspersky Security Network in Extended KSN mode (the **Use of Kaspersky Security Network (KSN)** toggle switch is enabled and the **Use Extended KSN mode** check box is selected in the Web Console, the **Extended KSN mode** option is selected in the Administration Console), by accepting the terms and conditions of the Kaspersky Security Network Statement, you agree to automatically provide the following information to Kaspersky in addition to the information listed above.

Data provision when using Extended KSN mode with Kaspersky Endpoint Detection and Response Expert (on-premises) Integration

If you use Kaspersky Endpoint Security as part of Kaspersky Endpoint Detection and Response Expert (on-premises), as well as Kaspersky Security Network in Extended mode, by accepting the terms of Kaspersky Security Network Statement you agree to automatically provide Kaspersky with the following information, in addition to the listed above.

Data provision when using Kaspersky Endpoint Security in Basic mode or Endpoint Detection and Response Agent mode

If you use Kaspersky Endpoint Security in Standard mode or Endpoint Detection and Response Agent mode, as well as Kaspersky Security Network in Extended mode, by accepting the terms of Kaspersky Security Network Statement you agree to automatically provide Kaspersky with the following information, in addition to the listed above:

Data provided when integrating with Kaspersky Endpoint Detection and Response Optimum

Data transmitted together with *IOC Scan* task results

Kaspersky Endpoint Security automatically sends data about *IOC Scan* task results to Kaspersky Security Center.

IOC Scan task result data may contain the following information:

- Network information:
  - IP address from the Address Resolution Protocol (ARP) table
  - MAC address from the Address Resolution Protocol table
  - Type and name of DNS record
  - IP address of the protected device

    - MAC address of the protected device
    - IP address and port of the remote connection
    - IP address of the local network adapter
    - Number of the open port on the local adapter
    - Protocol number according to the Internet Assigned Numbers Authority (IANA) standard
- Information about processes:
    - Process name
    - Process arguments
    - Path to the executable file of the process
    - Process ID (PID)
    - Parent process ID
    - Name of the user that started the process
    - Date and time when the process was started
- Information about services:
    - Service name
    - Service description
    - Path and name of the service executable file
    - Service ID
    - Service type (kernel driver, adapter, etc.)
    - Service status
    - Service starting mode
    - Name of the user that started the service
- Information about the file system:
    - Volume name
    - Volume letter
    - Volume type

- Information about the operating system:
  - Name and version of the operating system
  - Network name of the protected device
  - Domain or group to which the device belongs
- Information about web activity:
  - Browser name
  - Browser version
  - Time of the last access to the web resource
  - Web address of the HTTP request
  - Name of the user that made the HTTP request
  - Name of the process that made the HTTP request
  - Path to the executable file of the process that made the HTTP request
  - ID of the process that made the HTTP request
  - HTTP referer (web address of the HTTP request source)
  - Web address of the requested resource
  - User agent of the processed web request (HTTP User-Agent)
  - HTTP request execution time
  - Unique ID of the process that made the HTTP request

Data for creating a threat development chain

Data for creating a threat development chain may contain the following information:

- General information about the alert:
  - Alert date and time
  - Object name
  - Scan mode
  - Status of the last action related to the alert
  - Reason why the alert processing failed

- Information about the processed object:
  - Process identifier
  - Parent process ID
  - Process file ID
  - Command line of the process
  - Name of the user that started the process
  - ID of the session in which the process was started
  - Type of the session in which the process was started
  - Integrity level of the processed object
  - Whether the user belongs to privileged groups
  - ID of the processed object
  - Full name of the processed object
  - ID of the protected device
  - Full name of the object (local file or web address)
  - MD5 and SHA256 checksums of the processed object
  - Type of the processed object
  - Date when the object was created and last modified
  - size of the object being processed;
  - file attributes of an object being processed;
  - Information about the organization that signed the object
  - Verification result of the digital certificate of the object
  - Security identifier (SID) of the object
  - Time zone ID of the object
  - Web address from which the object was downloaded (for files only)
  - Name of the application that downloaded the file
  - MD5 and SHA256 checksums of the application that downloaded the file
  - Name of the application that last modified the file
  - MD5 and SHA256 checksums of the application that last modified the file

- Number of times the processed object was started
- Date and time of the first start of the processed object
- Unique ID of the file
- Full name of the file (local file or web address)
- Web address of the processed web request
- Source of the processed web request's links (HTTP referer)
- User agent of the processed web request
- Type of the processed web request (GET or POST)
- Local IP port of the processed web request
- Remote IP port of the processed web request
- Connection direction (inbound or outbound) of the processed web request
- ID of the process into which the malicious code was injected

Data provided when integrating with the Kaspersky Endpoint Detection and Response (KATA) component

When integrating Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform solution, Kaspersky Endpoint Security stores the following information, which may contain personal and confidential data:

- Addresses of Central Node servers that provide interaction with Kaspersky Endpoint Detection and Response (KATA) (hereinafter also referred to as *KATA servers*).
- Public key of the certificate of the server for integrating with Kaspersky Endpoint Detection and Response (KATA)
- Client certificate for integrating with Kaspersky Endpoint Detection and Response (KATA)
- Credentials for authenticating on the proxy server.
- Settings for the frequency of synchronization with the KATA server and settings for sending data to the KATA server
- Status of the connection with the KATA server and information about client certificate and server certificate errors
- Settings of tasks received from KATA servers:
  - Task start schedule settings
  - Names and passwords of accounts that must be used to start tasks

    - Versions of settings
    - Type of service start
    - Names of services
    - Command line (including arguments) used to start the process
    - MD5 and SHA256 hashes of objects
    - Paths to objects
    - IOC files
- Isolation settings in accordance with which a device is blocked from connecting to other devices except those specified in the exclusions

When integrating Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security stores the following information and may send it to the KATA server:

- Information for synchronization requests to the EDR Expert (on-premise) component:
    - Unique identifier
    - Base part of the server address
    - Device name
    - IP address of the device
    - MAC address of the device
    - Local time on the device
    - Name and version of the operating system installed on the device
    - Version of Kaspersky Endpoint Security
    - Release date of the application databases being used
    - License key status
- Information from requests to the EDR Expert (on-premise) component in task execution reports:
    - IP address of the device
    - Unique identifier
    - Base part of the server address
    - MAC address of the device
    - Task execution errors and return codes
    - Task completion statuses

- Task completion time
- Versions of task settings used
- Information about processes started or stopped on the device at the server's request: PID and UniquePID, error code, MD5 and SHA256 checksums of objects
- Files requested by the server
- Information about errors while getting information about objects: full name of the object that was processed with an error; error code
- Network isolation status
- For IOCs, scan results are returned (whether each indicator was detected, objects found, and information about which branch of the indicator was detected).
- For objects in which IOCs were detected, different values are returned depending on the type of indicator:
  - ArpEntry: IP address from the ARP table (including ipv6), physical address from the ARP table.
  - File: MD5 hash of the file, SHA256 hash of the file, full file name (including path), file size.
  - Port: remote IP address and port used to established a connection during scan; IP address and port of the local adapter; protocol type (TCP, UDP, IP, RAWIP).
  - Process: process name; process arguments; path to the process file; system PID of the process; system PID of the parent process; name of the user that started the process; date and time the process started.
  - SystemInfo: OS name; OS version; network name of the device without a domain; domain or workgroup.
  - User: user name.
- For quarantined objects:
  - File path
  - File size
  - File ID that was assigned when quarantining
  - Original file deletion flag
- For files obtained from Quarantine:
  - File ID that was assigned when quarantining
- For prevented executions of executable files or scripts:
  - Process ID
  - Parent process ID
  - System ID

        - Logon session ID
        - Process status
        - Date and time of execution interception
    - For prohibited document openings by office applications:
        - Process ID
        - File ID
        - Date and time of execution interception
- Information about files:
    - Unique ID of the file
    - MD5 hash of the object
    - File contents
- Data in telemetry packets:
    - Information about files:
        - Unique ID of the file
        - File path
        - File name
        - File size
        - File attributes
        - Creation date and time of the file
        - Last modification date and time of the file
        - MD5 and SHA256 hashes of the object
        - Information (name and ID) about the user and group that own the file
    - Information about running processes:
        - Process file ID
        - Process ID
        - Command line options that the process was started with
        - Session ID

    - Date and time when the process was started
    - Information (name and ID) about the user and group that started the process
- Information about the process gaining access to the memory of another process:
    - Process ID
    - Method and address of injection.
    - Command line (including arguments) used to modify the process.
    - System call arguments of the process
- Information about detected and processed threats:
    - Name of the detected threat and the technology that detected the threat, according to the Kaspersky classification
    - Application database version
    - Web address from which the infected object was downloaded
    - Threat processing status
    - The reason why the threat cannot be eliminated
    - Unique ID of the threat file
- File modification data:
    - Unique ID of the modified file
    - Unique ID of the process that made the changes
    - Information about the modification
- Data about changes in the system:
    - Unique ID of the process that made the changes
    - Information about the change that occurred
- User logon information:
    - Session ID
    - User information (name and ID)
    - IP address of the device from which the session was established
- Data about processes being terminated: unique ID of the process
- Information about loading a library into the address space of the process: the ID of the loaded library

- Information about an established network connection:
  - Local IP address
  - Remote IP address
  - Direction of the connection
  - Protocol
- Information about the process that is listening for external network connections on a certain port:
  - Local address (port and IP address)
  - Protocol
- DNS server query information:
  - Domain name of the queried resource
  - IP address of the queried resource
  - DNS server IP address
  - Query type

The information listed here can also be saved in trace files and dump files.

Data provided when integrating with the Kaspersky Endpoint Detection and Response Expert (on-premises) component

When integrating Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Expert (on-premises), Kaspersky Endpoint Security stores the following information, which may contain personal and confidential data:

- List of servers for integrating with Kaspersky Endpoint Detection and Response Expert (on-premises).
- Public key of the certificate of the server providing integration with Kaspersky Endpoint Detection and Response Expert (on-premises).
- Client certificate for integrating with Kaspersky Endpoint Detection and Response Expert (on-premises).
- Credentials for authenticating on the proxy server.
- Settings for the frequency of synchronization with the server that is responsible for the integration with Kaspersky Endpoint Detection and Response Expert (on-premises) and data transmission settings for this server.
- The status of the connection to the server that handles integration with Kaspersky Endpoint Detection and Response Expert (on-premises), and information about client and server certificate errors.

- Parameters of tasks coming from servers for integrating with Kaspersky Endpoint Detection and Response Expert (on-premises):
  - Task start schedule settings
  - Names and passwords of accounts that must be used to start tasks
  - Versions of settings
  - Type of service start
  - Names of services
  - Command line (including arguments) used to start the process
  - MD5 and SHA256 hashes of objects
  - Paths to objects
  - IOC files
- Isolation settings in accordance with which a device is blocked from connecting to other devices except those specified in the exclusions

When the Kaspersky Endpoint Security application is integrated with Kaspersky Endpoint Detection and Response Expert (on-premises), the application saves and can transmit the following data to the integration server:

- Information for synchronization requests to the EDR Expert (on-premises) component:
  - Unique identifier
  - Base part of the server address
  - Device name
  - IP address of the device
  - MAC address of the device
  - Local time on the device
  - Name and version of the operating system installed on the device
  - Version of Kaspersky Endpoint Security
  - Release date of the application databases being used
  - License key status
- Information from requests to the EDR Expert (on-premises) component in task execution reports:
  - IP address of the device
  - Unique identifier
  - Base part of the server address

- MAC address of the device
- Task execution errors and return codes
- Task completion statuses
- Task completion time
- Versions of task settings used
- Information about processes started or stopped on the device at the server's request: PID and UniquePID, error code, MD5 and SHA256 checksums of objects
- Files requested by the server
- Information about errors while getting information about objects: full name of the object that was processed with an error; error code
- Network isolation status
- For IOCs, scan results are returned (whether each indicator was detected, objects found, and information about which branch of the indicator was detected).
- For YARA rules, search results are returned (whether the rule was triggered or not, found objects, and information about which rule was triggered).
- For objects in which IOCs were detected, and YARA rules, different values are returned depending on the type:
  - ArpEntry: IP address from the ARP table (including ipv6), physical address from the ARP table.
  - File: MD5 hash of the file, SHA256 hash of the file, full file name (including path), file size.
  - Port: remote IP address and port used to established a connection during scan; IP address and port of the local adapter; protocol type (TCP, UDP, IP, RAWIP).
  - Process: process name; process arguments; path to the process file; system PID of the process; system PID of the parent process; name of the user that started the process; date and time the process started.
  - SystemInfo: OS name; OS version; network name of the device without a domain; domain or workgroup.
  - User: user name.
- For quarantined objects:
  - File path
  - File size
  - File IDs that were assigned when quarantining
  - Original file deletion flag
- For files received in, restored, or deleted from Quarantine:
  - File IDs that were assigned when quarantining

- For prevented executions of executable files or scripts:
  - Process ID
  - Parent process ID
  - System ID
  - Logon session ID
  - Process status
  - Date and time of execution interception
- For prohibited document openings by office applications:
  - Process ID
  - File ID
  - Date and time of execution interception
- List of files in the specified directory:
  - File name
  - Absolute path to file
  - File size
  - File type
  - Name and ID of the owner user and owner group
  - File access permissions
  - Special file system flags applied to each file
  - File metadata
  - Number of hard links to the file
  - File creation, modification, and last access times
- List of running processes on the device:
  - Process name
  - Process start time
  - Process status
  - Process ID (PID) and parent process ID
  - Current working directory of the process

    - Command line options that the process was started with
    - Environment variables
    - Path to the executable file of the process
    - Session ID of the user that started the process
    - IDs of the user and group that started the process
    - IDs of the user and group with whose rights the process has access to files and resources in the system
  - List of autorun points:
    - Type of the autorun point
    - File name
    - Absolute path to file
    - File access permissions
    - Special file system flags applied to each file
    - Name and ID of the owner user and owner group
    - File creation, modification, and last access times
  - Process memory image:
    - Process name
    - Full path to process file
    - Process dump file
    - Size of the process dump file
  - Device memory image: dump file of the device RAM
  - Device disk image
- Information about files:
  - Unique ID of the file
  - MD5 hash of the object
  - File contents

- Data in telemetry packets:
  - Data for telemetry events:
    - Event ID.
    - The number of the event in the sequence of the telemetry packets being sent.
    - Event type.
    - Event time.
  - Information about the protected device:
    - Name of the protected device.
    - ID of the protected device in Kaspersky Security Center.
    - ID of the protected device in Kaspersky Endpoint Detection and Response Expert (on-premises).
    - Name, version, family of the operating system installed on the protected device.
    - Startup and shutdown times of the operating system installed on the protected device.
  - Information about files:
    - Unique ID of the file
    - File path
    - File name
    - File size
    - File attributes
    - Creation date and time of the file
    - Last modification date and time of the file
    - MD5 and SHA256 hashes of the object
    - Information (name and ID) about the user and group that own the file
  - Information about running processes:
    - Process file ID
    - Process ID
    - Command line options that the process was started with
    - Session ID

    - Date and time when the process was started
    - Information (name and ID) about the user and group that started the process
- Information about the process gaining access to the memory of another process:
    - Process ID
    - Method and address of injection.
    - Command line (including arguments) used to modify the process.
    - System call arguments of the process
- Information about detected and processed threats:
    - Name of the detected threat and the technology that detected the threat, according to the Kaspersky classification
    - Release date and version of the application databases
    - Web address from which the infected object was downloaded
    - Threat processing status
    - The reason why the threat cannot be eliminated
    - Unique ID of the threat file
- File modification data:
    - Unique ID of the modified file
    - Unique ID of the process that made the changes
    - Information about the modification
- Data about changes in the system:
    - Unique ID of the process that made the changes
    - Information about the change that occurred
- User logon information:
    - Session ID
    - User information (name and ID)
    - IP address of the device from which the session was established
- Data about processes being terminated: unique ID of the process
- Information about loading a library into the address space of the process: the ID of the loaded library

- Information about establishing and terminating a network connection:
  - Local IP address
  - Remote IP address
  - Direction of the connection
  - Protocol
  - Connection establishment time
  - Connection termination time
  - Connection duration
  - Bytes sent during the connection
  - Bytes received during the connection
- Information about the process that is listening for external network connections on a certain port:
  - Local address (port and IP address)
  - Protocol
- DNS server query information:
  - Domain name of the queried resource
  - IP address of the queried resource
  - DNS server IP address
  - Query type
- Information about connected external devices:
  - Operation type (device connection)
  - Device type
  - Unique device ID
  - Device name
  - Device path
- Information about the application and its modules:
  - Application version.
  - Time when the application was installed, started, stopped, or uninstalled.
  - Initiator of the action with the application.

    - Reason for stopping the application in case of an abnormal stop.
    - Return codes in case of an abnormal stop.
- Information about interaction with task schedulers (task creation and deletion):
    - Task name.
    - Path to the scheduled command.
    - Task launch schedule.
    - Name of the user that created the task.
    - Name of the user that started the task.
    - Name of the user that deleted the task.
- Information about service creation, deletion, and modification:
    - Service name (including the previous name if changed)
    - Service type (including the previous type if changed)
    - Path to the executable file (including the previous path if changed)
    - Service dependencies (including the previous dependencies if changed)
    - Name of the user that started the service (including the previous user name if changed)
    - Display name of the service (including the previous display name if changed)
    - Name of the user that created, deleted, or modified the service
    - Deferred deletion flag
- Information about console input:
    - ID and type of the process that initiated the console input
    - Content of the console input
- Information about mounted devices:
    - System name of the volume
    - Mount point

- Information about changes in the process memory:
  - System call arguments of the process
  - Information about the process that performed the code injection and about its parent process
    - Process ID and unique ID of the process and parent process
    - The command line that was used to start the process and the parent process
    - Environment variables of the process
    - Type of user account under which the process and parent process were started
    - System call that was used to spawn the process
    - IDs of the user and group that started the process
    - Name and full name of the process and parent process
    - Full path to the process and parent process
    - MD5 and SHA256 hashes of the process and parent process
    - Session ID
    - Name, domain name, and ID of the user that started the process and parent process
  - Information about the process through which the process that performed the code injection was loaded
    - Unique ID of the process through which the process was loaded
    - Name and full name of the file through which the process was loaded
    - Full path to the process through which the process was loaded
    - MD5 hash of the process through which the process was loaded
  - Information about the process that is the initiator of the process
    - Process ID and unique ID of the process that is the initiator of the process
    - Command line of the process that is the initiator of the process
    - Name and domain name of the user that started the process that is the initiator of the process
    - Name and full name of the process that is the initiator of the process
    - Full path to the process that is the initiator of the process
    - MD5 and SHA256 hashes of the process that is the initiator of the process

The information listed here can also be saved in trace files and dump files.

Data provided when integrating with the Kaspersky Endpoint Detection and Response Expert (cloud) component

When integrating Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Expert (cloud), Kaspersky Endpoint Security stores the following information, which may contain personal and confidential data:

- List of servers for integrating with Kaspersky Endpoint Detection and Response Expert (cloud).
- Addresses of the telemetry and response server tunnels for Kaspersky Endpoint Detection and Response Expert (cloud).
- Server certificate for integrating with Kaspersky Endpoint Detection and Response Expert (cloud).
- Client certificate for integrating with Kaspersky Endpoint Detection and Response Expert (cloud).
- Settings for the frequency of synchronization with the server that is responsible for the integration with Kaspersky Endpoint Detection and Response Expert (cloud) and data transmission settings for this server.
- The status of the connection to the server that handles integration with Kaspersky Endpoint Detection and Response Expert (cloud), and information about client and server certificate errors.
- Parameters of tasks coming from servers for integrating with Kaspersky Endpoint Detection and Response Expert (cloud):
  - Task start schedule settings
  - Names and passwords of accounts that must be used to start tasks
  - Versions of settings
  - Type of service start
  - Names of services
  - Command line (including arguments) used to start the process
  - MD5 and SHA256 hashes of objects
  - Paths to objects
  - IOC files
- Isolation settings in accordance with which a device is blocked from connecting to other devices except those specified in the exclusions

When the Kaspersky Endpoint Security application is integrated with Kaspersky Endpoint Detection and Response Expert (cloud), the application saves and can transmit the following data to the integration server:

- Information for synchronization requests to the EDR Expert (cloud) component:
  - Unique identifier
  - Base part of the server address
  - Device name
  - IP address of the device
  - MAC address of the device
  - Local time on the device
  - Name and version of the operating system installed on the device
  - Version of Kaspersky Endpoint Security
  - Release date of the application databases being used
  - License key status
- Information from requests to the EDR Expert (cloud) component in task execution reports:
  - IP address of the device
  - Unique identifier
  - Base part of the server address
  - MAC address of the device
  - Task execution errors and return codes
  - Task completion statuses
  - Task completion time
  - Versions of task settings used
  - Information about processes started on the device at the request of the server:
    - Process termination code
    - Unique ID of the standard output file of the process.
    - Unique ID of the standard error file of the process.

- Information about processes started or stopped on the device at the request of the server:
  - PID (system process ID).
  - UniquePID (unique identifier of the process)
  - Error code
- Copy of the file requested by the server, as well as the path to the file and its ID.
- Flag for deletion of the file after OS restart.
- Information about errors while getting information about objects: full name of the object that was processed with an error; error code
- Network isolation status
- For IOCs, scan results are returned (whether each indicator was detected, objects found, and information about which branch of the indicator was detected).
- For objects in which IoCs were detected, different values are returned depending on the type of indicator:
  - ArpEntry: IP address from the ARP table (including ipv6), physical address from the ARP table.
  - File: MD5 hash of the file, SHA256 hash of the file, full file name (including path), file size.
  - Port: remote IP address and port used to established a connection during scan; IP address and port of the local adapter; protocol type (TCP, UDP, IP, RAWIP).
  - Process: process name; process arguments; path to the process file; system PID of the process; system PID of the parent process; name of the user that started the process; date and time the process started.
  - SystemInfo: OS name; OS version; network name of the device without a domain; domain or workgroup.
  - User: user name.
- For quarantined objects:
  - File path
  - File size
  - File IDs that were assigned when quarantining
  - Original file deletion flag
- For files received in, restored, or deleted from Quarantine:
  - File IDs that were assigned when quarantining
- For prevented executions of executable files or scripts:
  - Process ID
  - Parent process ID

    - System ID
    - Logon session ID
    - Process status
    - Date and time of execution interception
- For prohibited document openings by office applications:
    - Process ID
    - File ID
    - Date and time of execution interception
- List of files in the specified directory:
    - File name
    - Absolute path to file
    - File size
    - File type
    - Name and ID of the owner user and owner group
    - File access permissions
    - Special file system flags applied to each file
    - File metadata
    - Number of hard links to the file
    - File creation, modification, and last access times
- List of running processes on the device:
    - Process name
    - Process start time
    - Process status
    - Process ID (PID) and parent process ID
    - Current working directory of the process
    - Command line options that the process was started with
    - Environment variables
    - Path to the executable file of the process

    - Session ID of the user that started the process
    - IDs of the user and group that started the process
    - IDs of the user and group with whose rights the process has access to files and resources in the system
- List of autorun points:
    - Type of the autorun point
    - File name
    - Absolute path to file
    - File access permissions
    - Special file system flags applied to each file
    - Name and ID of the owner user and owner group
    - File creation, modification, and last access times
    - MD5 hash and SHA-256 hash of the executable file or loadable module.
- Process memory image:
    - Name of the process memory image file.
    - Full path to process file
    - Unique ID of the process memory image file.
    - Size of the process memory image file.
- Device memory image:
    - Date and time when the dumping began.
    - Full path to dump file
    - Size of the device memory image file.
- Device disk image:
    - Date and time when the dumping began.
    - Array of full paths to the dump files
    - Size of the device disk image file.
    - Logical disk.
    - Physical disk.

- Data in telemetry packets:
  - Data for telemetry events:
    - Event ID.
    - The number of the event in the sequence of the telemetry packets being sent.
    - Event type.
    - Event time.
  - Information about the protected device:
    - Name of the protected device.
    - ID of the protected device in Kaspersky Security Center.
    - ID of the protected device in Kaspersky Endpoint Detection and Response Expert (on-premises).
    - Name, version, family of the operating system installed on the protected device.
    - Startup and shutdown times of the operating system installed on the protected device.
  - Information about files:
    - Unique ID of the file
    - File path
    - File name
    - File size
    - File attributes
    - Creation date and time of the file
    - Last modification date and time of the file
    - MD5 and SHA256 hashes of the object
    - Information (name and ID) about the user and group that own the file
  - Information about running processes:
    - Process file ID
    - Process ID
    - Command line options that the process was started with
    - Session ID

    - Date and time when the process was started
    - Information (name and ID) about the user and group that started the process
- Information about the process gaining access to the memory of another process:
    - Process ID
    - Method and address of injection.
    - Command line (including arguments) used to modify the process.
    - System call arguments of the process
- Information about detected and processed threats:
    - Name of the detected threat and the technology that detected the threat, according to the Kaspersky classification
    - Release date and version of the application databases
    - Web address from which the infected object was downloaded
    - Threat processing status
    - The reason why the threat cannot be eliminated
    - Unique ID of the threat file
- File modification data:
    - Unique ID of the modified file
    - Unique ID of the process that made the changes
    - Information about the modification
- Data about changes in the system:
    - Unique ID of the process that made the changes
    - Information about the change that occurred
- User logon information:
    - Session ID
    - User information (name and ID)
    - IP address of the device from which the session was established
- Data about processes being terminated: unique ID of the process
- Information about loading a library into the address space of the process: the ID of the loaded library

- Information about establishing and terminating a network connection:
  - Local IP address
  - Remote IP address
  - Direction of the connection
  - Protocol
  - Connection establishment time
  - Connection termination time
  - Connection duration
  - Bytes sent during the connection
  - Bytes received during the connection
- Information about the process that is listening for external network connections on a certain port:
  - Local address (port and IP address)
  - Protocol
- DNS server query information:
  - Domain name of the queried resource
  - IP address of the queried resource
  - DNS server IP address
  - Query type
- Information about connected external devices:
  - Operation type (device connection)
  - Device type
  - Unique device ID
  - Device name
  - Device path
- Information about the application and its modules:
  - Application version.
  - Time when the application was installed, started, stopped, or uninstalled.
  - Initiator of the action with the application.

    - Reason for stopping the application in case of an abnormal stop.
    - Return codes in case of an abnormal stop.
- Information about interaction with task schedulers (task creation and deletion):
    - Task name.
    - Path to the scheduled command.
    - Task launch schedule.
    - Name of the user that created the task.
    - Name of the user that started the task.
    - Name of the user that deleted the task.
- Information about service creation, deletion, and modification:
    - Service name (including the previous name if changed)
    - Service type (including the previous type if changed)
    - Path to the executable file (including the previous path if changed)
    - Service dependencies (including the previous dependencies if changed)
    - Name of the user that started the service (including the previous user name if changed)
    - Display name of the service (including the previous display name if changed)
    - Name of the user that created, deleted, or modified the service
    - Deferred deletion flag
- Information about console input:
    - ID and type of the process that initiated the console input
    - Content of the console input
- Information about mounted devices:
    - System name of the volume
    - Mount point

- Information about changes in the process memory:
  - System call arguments of the process
  - Information about the process that performed the code injection and about its parent process
    - Process ID and unique ID of the process and parent process
    - The command line that was used to start the process and the parent process
    - Environment variables of the process
    - Type of user account under which the process and parent process were started
    - System call that was used to spawn the process
    - IDs of the user and group that started the process
    - Name and full name of the process and parent process
    - Full path to the process and parent process
    - MD5 and SHA256 hashes of the process and parent process
    - Session ID
    - Name, domain name, and ID of the user that started the process and parent process
  - Information about the process through which the process that performed the code injection was loaded
    - Unique ID of the process through which the process was loaded
    - Name and full name of the file through which the process was loaded
    - Full path to the process through which the process was loaded
    - MD5 hash of the process through which the process was loaded
  - Information about the process that is the initiator of the process
    - Process ID and unique ID of the process that is the initiator of the process
    - Command line of the process that is the initiator of the process
    - Name and domain name of the user that started the process that is the initiator of the process
    - Name and full name of the process that is the initiator of the process
    - Full path to the process that is the initiator of the process
    - MD5 and SHA256 hashes of the process that is the initiator of the process

The information listed here can also be saved in trace files and dump files.

Data provided when integrating with the Kaspersky Network Detection and Response (KATA) component

When integrating Kaspersky Endpoint Security with Kaspersky Network Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform solution, Kaspersky Endpoint Security stores the following information, which may contain personal and confidential data:

- NDR server addresses
- Public key of the server certificate for integration with Kaspersky Network Detection and Response (KATA)
- Client certificate for integration with Kaspersky Network Detection and Response (KATA)
- Credentials for authenticating on the proxy server.
- Settings for the frequency of synchronization with the NDR server and settings for sending data to the NDR server
- NDR server connection status and information about errors related to the client certificate and server certificate

When Kaspersky Endpoint Security is integrated with the Kaspersky Network Detection and Response (KATA) component, the Kaspersky Endpoint Security application stores and sends the following data to the NDR server:

- Data from synchronization requests to the NDR server:
  - Unique identifier
  - Base part of the server address
  - Device name
  - IP address of the device
  - MAC address of the device
  - Local time on the device
  - Name, family and version of the operating system installed on the device
  - Version of Kaspersky Endpoint Security
  - Release date of the application databases being used
  - License key status
  - Model and manufacturer of the user's device

- Data in telemetry packets:
  - Information about the device and users:
    - Device name and time on the device
    - Family, name, and version of the operating system
    - Information about network interfaces (description, list of IP addresses with subnet mask, MAC address, metric number, DNS domain name, routing information, listening port numbers)
    - Device internal unique ID
    - User names and IDs
    - User group names and IDs
  - Information about the Kaspersky Endpoint Security application:
    - Name and version of the application
    - Date of the last application update
    - Information about license keys (serial number, type, license validity period, key status)
    - Application database version
    - List of supported API versions
  - Information about established connections:
    - Local IP address, port and MAC address
    - Remote IP address, port and MAC address
    - Gateway IP address.
    - Protocol type (according to IANA), protocol number and EtherType
    - Number of received and sent packages
  - Information about processed files:
    - File name and unique ID
    - File type and size
    - Full path to the file image
    - File system attribute mask
    - The time when the file was created and modified

    - Checksums (MD5 and SHA256)
    - File privileges, including inherited and effective
- Information about running and terminating processes:
    - Process UID and PID
    - Process type.
    - Session ID
    - Executed command
    - Environment variables
- Information about detected and processed threats:
    - Name of the detected threat and the technology that detected the threat, according to the Kaspersky classification
    - Application database version
    - Web address from which the infected object was downloaded
    - Threat processing status
    - The reason why the threat cannot be eliminated

The information listed here can also be saved in trace files and dump files.

Data provided when integrating with Kaspersky Unified Monitoring and Analysis Platform

When integrating Kaspersky Endpoint Security with Kaspersky Unified Monitoring and Analysis Platform, Kaspersky Endpoint Security stores the following information, which may contain personal and confidential data:

- KUMA server addresses
- Public key of the server certificate for integration with Kaspersky Unified Monitoring and Analysis Platform (except when the UDP protocol is used to connect to the KUMA server)
- Client certificate for integration with Kaspersky Unified Monitoring and Analysis Platform
- Credentials for authenticating on the proxy server.
- Settings for the frequency of synchronization with the KUMA server and settings for sending data to the KUMA server
- KUMA server connection status and information about errors related to the client certificate and server certificate

When integrating Kaspersky Endpoint Security with Kaspersky Unified Monitoring and Analysis Platform, the Kaspersky Endpoint Security application saves and transmits the following data to the KUMA server in telemetry packets:

- Information about file modifications:
  - Unique ID of the file before the modification
  - Unique ID of the modified file
  - Unique ID of the process that made the changes
  - Type and flag of the file operation
  - Date and time the file was modified
- Information about running and terminating processes:
  - Process file ID
  - Process UID and PID
  - Command line options that the process was started with
  - Session ID
  - Date and time when the process was started
  - Information (name and ID) about the user and group that started the process
- Information about events in the event log:
  - Date and time of event
  - UID of the process associated with the event
  - Type and description of the event
  - Result of performing the operation

Information about third-party code

Information about third-party code is contained in the file legal_notices.txt located in the application installation folder.

Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Adobe, Acrobat, Flash, and Shockwave are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD64 is a trademark or registered trademark of Advanced Micro Devices, Inc.

Amazon is a trademark of Amazon.com, Inc. or its affiliates.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

AutoCAD is a trademark or registered trademark of Autodesk, Inc., and/or its subsidiaries and/or affiliates in the USA and/or other countries.

Borland is trademark or registered trademark of Borland Software Corporation.

dBase is a trademark of dataBased Intelligence, Inc.

FireWire is a trademark of Apple Inc.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Ubuntu and LTS are registered trademarks of Canonical Ltd.

XenServer is either a registered trademark or trademark of Cloud Software Group, Inc., and/or its subsidiaries in the United States and/or other countries.

Cloudflare, the Cloudflare logo, and Cloudflare Workers are trademarks and/or registered trademarks of Cloudflare, Inc. in the United States and other jurisdictions.

The Grafana Word Mark and Grafana Logo are either registered trademarks/service marks or trademarks/service marks of Coding Instinct AB, in the United States and other countries and are used with Coding Instinct's permission. We are not affiliated with, endorsed or sponsored by Coding Instinct, or the Grafana community.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights in other terms used herein.

Chrome, Chromium, Google Chrome, Google Public DNS are trademarks of Google LLC.

HUAWEI, EulerOS, and FusionSphere are trademarks of Huawei Technologies Co., Ltd.

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

Microsoft, Microsoft Edge, Active Directory, Hyper-V, Outlook, Visual Basic, Visual FoxPro, Visual C++, PowerPoint, Excel, Internet Explorer, Windows, and Windows Server are trademarks of the Microsoft group of companies.

OpenStack is a registered trademark of the OpenStack Foundation in the United States and other countries.

Oracle, Java, and JavaScript are registered trademarks of Oracle and/or its affiliates.

Python is a trademark or registered trademark of the Python Software Foundation.

Red Hat Enterprise Linux, CentOS, and Fedora 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.

Kubernetes is a registered trademark of The Linux Foundation in the United States and other countries.

Rocky Linux is a trademark of The Rocky Enterprise Software Foundation.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

Zabbix is a registered trademark of Zabbix SIA.