kaspersky

Kaspersky Endpoint Security for Linux

Contents

Kaspersky Endpoint Security 12.1 for Linux

Kaspersky Endpoint Security 12.1 for Linux ("Kaspersky Endpoint Security," "Application") designed to protect devices running Linux® operating systems against various types of threats, including network and scam attacks.

The application allows you to protect both physical devices and virtual machines. You can use Kaspersky Endpoint Security as part of Kaspersky Security for Virtualization Light Agent to protect virtual machines running Linux guest operating systems.

The following functional components and tasks of the application provide the main functions of device protection and control:

- **File Threat Protection** prevents infection of the file system on the user device. The *File Threat Protection* component starts automatically when Kaspersky Endpoint Security is launched and scans all files that are opened, saved, and started in real time.

  You can also scan protected devices on demand using the following scan tasks:

  - **Malware Scan**. The application scans for the presence of malware in file system objects located on local disks of the device, as well as mounted and shared resources, which are accessed via SMB and NFS protocols. You can use this task to perform a full or custom scan of the device.

  - **Critical Areas Scan**. The application scans boot sectors, startup objects, process memory, and kernel memory.

- **Removable Drives Scan**. The *Removable Drives Scan* component allows you to monitor the connection of removable drives to the device in real time and scan a removable drive and its boot sectors for malware. Kaspersky Endpoint Security can scan the following removable drives: CDs, DVDs, Blu-ray discs, flash drives (including USB modems), external hard drives, and floppy disks.

- **Container scan**. The *Container Scan* component allows you to scan namespaces and running containers for malware in real time. Integration with Docker container management system, CRI-O framework, and Podman and runc utilities is supported. You can use the *Container Scan* task to scan containers and images on demand.

- **Web Threat Protection**. The *Web Threat Protection* component allows you to scan inbound traffic, prevent downloads of malicious files from the Internet, and block phishing, adware, and other malicious websites. Kaspersky Endpoint Security can scan encrypted connections.

- **Network Threat Protection**. The *Network Threat Protection* component allows you to scan inbound network traffic for activity that is typical for network attacks.

- **Firewall Management**. The *Firewall Management* component allows you to monitor the firewall settings of the operating system and filter all network activity in accordance with the network packet rules that you have configured.

- **Anti-Cryptor**. The *Anti-Cryptor* component allows you to scan remote devices' calls to files located in local directories with network access via SMB/NFS protocols and protect files from remote malicious encryption.

- **Device Control**. The *Device Control* component allows you to manage user access to the 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. User access to devices is governed by access regimes and access rules that you have configured.

- **Application Control**. The *Application Control* component allows you to manage the launch of applications on user devices. This reduces the risk of device infection by restricting access to applications. Application launching is regulated by the Application Control rules that you have configured.

- **Inventory**. The *Inventory* task provides information about all applications executable files stored on the client devices. This information can be useful, for example, for creating Application Control rules.

- **Web Control**. The *Web Control* component controls user access to web resources. This allows you to reduce traffic consumption and reduce inappropriate use of working 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.

- **Behavior Detection**. The *Behavior Detection* component allows you to monitor for any malicious activity from applications in the operating system. When malicious activity is detected, Kaspersky Endpoint Security can terminate the process of the application that performs malicious activity.

- **System Integrity Monitoring** allows you to track changes to files and directories of the operating system. The *System Integrity Monitoring* component monitors the actions performed with objects from the monitoring scope specified in the component settings in real time. You can use the *System Integrity Check* task to check the integrity of the system on demand. The check is performed by comparing the current states of objects included in the monitoring scope with their initial states, which were previously established as a baseline.

Kaspersky Endpoint Security allows you to detect infected objects and neutralize the threats detected in them. For this, the application can use:

- Application databases to detect and disinfect infected files. During the scan process, the application analyzes each file for the presence of a threat: it compares the file code with the code of a specific threat and looks for possible matches.

- Kaspersky Security Network. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Endpoint Security to various threats, improves the performance of some protection components, and reduces the likelihood of false positives.

Prior to disinfection or removal, Kaspersky Endpoint Security saves backup copies of files in the Backup located on the device. If after disinfection, you partially or completely lose access to important information in a disinfected file, you can restore the file from the copy.

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 reset.

Kaspersky Endpoint Security can operate in Notify-only mode. *Notify-only mode* is an operation mode for the application in which, if a threat is detected, application components and tasks do not attempt to disinfect or delete malicious objects, deny access or block the activity of applications. Instead, the application only informs the user about the detected threat.

Kaspersky Endpoint Security supports integration with other Kaspersky solutions to expand the capabilities of the application:

- Integration with Kaspersky Managed Detection and Response enables continuous search, detection and elimination of threats aimed at your organization.

- Integration with Kaspersky Endpoint Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform ensures the protection of your organization's IT infrastructure and prompt detection of threats, including zero-day attacks, targeted attacks, and advanced persistent threats.

- Integration with Kaspersky Endpoint Detection and Response Optimum 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.

You can use Kaspersky Endpoint Security as a container application (hereinafter also referred to as KESL container) for embedding into external systems in order to scan container images in repositories.

The KESL container functionality is not supported if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments.

To keep the application up to date, additional application functions are provided:

- Activating the application with a key file or activation code.

  If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, activation is performed on the Protection Server (a component of Kaspersky Hybrid Cloud Security for Virtualization Light Agent).

- Updating the databases and application modules from Kaspersky update servers, via the Administration Server, or from a user-specified source on schedule and on demand.

  If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the application receives updates of databases and application modules from the Protection Server (a component of Kaspersky Hybrid Cloud Security for Virtualization Light Agent).

- User access control for the application functions according to the user roles.
- Notification of the administrator about events that occurred while the application was running.
- Integrity check of application components using the integrity check tool.

You can manage Kaspersky Endpoint Security using the following methods:

- Using Kaspersky Security Center through the Kaspersky Security Center Web Console, Kaspersky Security Center Cloud Console, or the Administration Console.
- Using control commands from the command line.
- Using a graphical user interface.

  If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, it is not possible to manage the application using Kaspersky Security Center Cloud Console and the graphical user interface.

About Kaspersky Endpoint Security usage modes

You can use Kaspersky Endpoint Security in one of the following modes:

- In standard mode to protect workstations and servers ("Standard mode"). Kaspersky Endpoint Security is used as a standalone application for protecting devices running Linux operating systems.

- In Light Agent mode to protect virtual environments as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent ("Light Agent mode"). Kaspersky Endpoint Security is used as the Light Agent component of the Kaspersky Hybrid Cloud Security for Virtualization Light Agent solution to protect virtual machines running Linux guest operating systems.

The application is used in Standard mode by default.

If you want to use the application in Light Agent mode, you need to do the following:

1. Install Kaspersky Endpoint Security on each virtual machine that needs to be protected using Kaspersky Hybrid Cloud Security for Virtualization Light Agent. You can also install the application on a virtual machine template.

   During installation, you must specify that the application will be used in Light Agent mode in one of the following ways:

   - During the post-installation configuration of the application in interactive or automatic mode (if installed using the command line).
   - In the properties of the application installation package or in the autoinstall.ini configuration file that is included in the installation package (if installing using Kaspersky Security Center).

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

   When selecting Light Agent mode, you can also configure the following settings for Kaspersky Endpoint Security in Light Agent mode:

   - The role of the virtual machine that you want to protect, in the virtual infrastructure: server or 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.
   - VDI protection mode. It is recommended to enable this mode if you are installing the application on a virtual machine template that will be used to create temporary virtual machines. VDI protection mode optimizes the operation of Kaspersky Endpoint Security on temporary virtual machines.

2. Configure the settings for connecting Light Agent to SVMs and the settings for connecting Light Agent to the Integration Server.

   Kaspersky Endpoint Security in Light Agent mode interacts with other components of the Kaspersky Hybrid Cloud Security for Virtualization Light Agent solution: the Integration Server and the Protection Server installed on the SVM (for more information, see the Kaspersky Endpoint Security for Virtualization Light Agent Help). To interact with the Protection Server, Kaspersky Endpoint Security establishes and maintains a connection to the SVM on which this Protection Server is installed.

   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.

   You can configure the connection settings in the properties of a Kaspersky Endpoint Security policy using Kaspersky Security Center Administration Console or using Kaspersky Security Center Web Console.

You can obtain information about application operation settings in Light Agent mode, as well as information about the connection to the Integration Server and SVMs, by using the following application commands: `kesl-control --ksvla-info`, `kesl-control --viis-info` and `kesl-control --svm-info`.

Information about the application usage mode is displayed in Kaspersky Security Center in the properties of Kaspersky Endpoint Security on the managed device in the **Components** section. Information is displayed in the **Light Agent mode for protecting virtual environments** line as follows:

- The *Running* status means that the application is being used in Light Agent mode.

- The *Not installed* status means that the application is being used in Standard mode.

About activating the application in Light Agent mode

If Kaspersky Endpoint Security is used in Light Agent mode, the application does not need to be activated separately. You only activate Kaspersky Security for Virtualization Light Agent. Activation is performed on the Protection Server side (a component of Kaspersky Security for Virtualization Light Agent) by adding the license key on the SVM. For more details, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

To activate the Kaspersky Endpoint Detection and Response Optimum functionality, you also need to add an EDR Optimum license key to the SVM. Licenses for activating components of the Kaspersky Hybrid Cloud Security for Virtualization Light Agent solution do not include this functionality.

After activating the solution and connecting the Light Agent to the SVM, the Protection Server component sends license information to the Light Agent. When selecting an SVM to connect to, Light Agent considers, among other settings, the type of license key added to the SVM. The Light Agent does not connect to the SVM if the type of key added to the SVM does not match the role of the protected virtual machine in the virtual infrastructure (server or workstation). For more details, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

You can view information about the license used to activate Light Agent for Linux on the protected virtual machine with the Light Agent using the `kesl-control -L --query` command.

License keys cannot be managed using the *Add Key* task or via the Kaspersky Endpoint Security command for adding and deleting license keys.

About updating application databases and modules in Light Agent mode

Kaspersky Endpoint Security in Light Agent mode uses special anti-malware databases that are required for the application to work as part of Kaspersky Security for Virtualization Light Agent. Kaspersky Endpoint Security receives application database and module updates from the Protection Server. For more details, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

Databases and modules on protected virtual machines are updated using a special *Update* local task of Kaspersky Endpoint Security, where the folder on the SVM is specified as the update source. The update task starts automatically. You cannot delete this task or change its settings.

Update sources other than a folder on SVMs are not supported. The use of group update tasks is not supported.

The last anti-malware database update is also rolled back on the Protection Server side. After rolling back the application database and module update on the SVMs, a special *Update* local task is automatically started on the protected virtual machine. Completing the task causes the Light Agent to return to using the previous set of anti-malware databases.

The use of *Rollback* local and group tasks of Kaspersky Endpoint Security is not supported.

Other features of using the application in Light Agent mode

If Kaspersky Endpoint Security is used in Light Agent mode:

- The KESL container functionality is not supported.
- 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.
- Integration with Kaspersky Symphony XDR is not supported.

Distribution kit

You can download the files that are included in the Kaspersky Endpoint Security distribution kit, as well as the files needed to remotely install the application using Kaspersky Security Center, on the Kaspersky website.

The distribution kit includes Kaspersky Endpoint Security installation package containing the following files:

- kesl-12.1.0-<build number>.i386.rpm, kesl_12.1.0-<build number>_i386.deb

  Contain the main application files. Packages can be installed to 32-bit operating systems based on the type of package manager.

- kesl-12.1.0-<build number>.x86_64.rpm, kesl_12.1.0-<build number>_amd64.deb

  Contain the main application files. Packages can be installed to 64-bit operating systems based on the type of package manager.

- kesl-12.1.0-<build number>.aarch64.rpm, kesl_12.1.0-<build number>_arm64.deb

  Contain the main application files. Packages for the relevant package manager can be installed on 64-bit operating systems for the Arm® architecture.

- kesl-gui-12.1.0-<build number>.i386.rpm, kesl-gui_12.1.0-<build number>_i386.deb

  Contain the files of the application graphical user interface. Packages can be installed to 32-bit operating systems based on the type of package manager.

- kesl-gui-12.1.0-<build number>.x86_64.rpm, kesl-gui_12.1.0-<build number>_amd64.deb

  Contain the files of the application graphical user interface. Packages can be installed to 64-bit operating systems based on the type of package manager.

- kesl-gui-12.1.0-<build number>.aarch64.rpm, kesl-gui_12.1.0-<build number>_arm64.deb

  Contain the files of the application graphical user interface. Packages for the relevant package manager can be installed on 64-bit operating systems for the Arm architecture.

- kesl-12.1.0.<build number>.zip

Contains the files used for remote application installation using Kaspersky Security Center, including license.<language ID> and ksn_license.<language ID> files.

> 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.

- docker-service-kesl64-12.1.0-<build number>.tgz

  Contains files for creating an image of a KESL container application.

- ksn_license.<language ID>

  Contains the text of the Statement on Kaspersky Security Network.

- license.<language ID

  Contains the text of the License Agreement. The License Agreement specifies the terms for using the application.

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 of your device, inaccessible and corrupted data, as well as enabling the sending of additional statistics to KSN.

Hardware and software requirements

This section contains the hardware and software requirements for Kaspersky Endpoint Security.

Hardware requirements

Kaspersky Endpoint Security has the following hardware requirements:

Minimum hardware requirements:

- Core ™ 2 Duo 1.86 GHz or faster processor
- swap partition at least 1 GB
- 1 GB of RAM for 32-bit operating systems, 2 GB of RAM for 64-bit operating systems
- 4 GB of free hard disk space for installation of the application and storage of temporary and log files
- When using a graphical user interface, the monitor must be capable of displaying windows 1000 pixels wide and 600 pixels high (if screen scaling is applied, these dimensions are also scaled)
- if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, a virtual network interface with a bandwidth of 100 Mbit/s

Minimum hardware requirements for the Arm architecture:

- Armv8.2-A Kunpeng 920 or Armv8-A Baikal-M (BE-M1000) processor or m-TrusT Terminal
- swap partition at least 1 GB
- 2 GB of RAM
- 3 GB of free hard disk space for installation of the application and storage of temporary and log files
- When using a graphical user interface, the monitor must be capable of displaying windows 1000 pixels wide and 600 pixels high (if screen scaling is applied, these dimensions are also scaled)

Using Kaspersky Endpoint Security in Light Agent mode to protect virtual environments is not supported on operating systems based on the Arm architecture.

Software requirements

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

- 32-bit operating systems:
  - Debian GNU/Linux 11.0 and later.
  - Debian GNU/Linux 12.0 and later.
  - Mageia™ 4.

    Integration of the Kaspersky Endpoint Security application with Kaspersky Endpoint Detection and Response (KATA) is not supported on devices running the Mageia 4 operating system.
  - ALT 8 SP Workstation (8.4).
  - ALT 8 SP Server (8.4).
  - ALT SP Workstation release 10.
  - ALT SP Server release 10.
- 64-bit operating systems:
  - AlmaLinux OS 8 and later.
  - AlmaLinux OS 9 and later.
  - AlterOS® 7.5 and later.
  - Amazon™ Linux 2.
  - Astra Linux Common Edition 2.12.

- Astra Linux Special Edition RUSB.10015-01 (operational update 1.5).
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.6).
- Astra Linux Special Edition RUSB.10015-01 (operational update 1.7).
- Astra Linux Special Edition RUSB.10015-16 (release 1) (operational update 1.6).

  Using Kaspersky Endpoint Security in Light Agent mode to protect virtual environments is not supported on devices running Astra Linux operating systems in mandatory access control and closed software environment modes.

The Astra Linux operating system in the "Mobile" mode is only supported on tablet computers (tablets) in desktop mode.

- CentOS 7.2 and later.
- CentOS Stream 8.
- CentOS Stream 9.
- Debian GNU/Linux 11.0 and later.
- Debian GNU/Linux 12.0 and later.
- EMIAS 1.0 and later.
- EulerOS 2.0 SP10.
- Kylin 10.
- Linux Mint 20.3 and up.
- Linux Mint 21.1 and later.
- openSUSE Leap 15.0 and later.
- Oracle Linux 7.3 and later.
- Oracle Linux 8.0 and later.
- Oracle Linux 9.0 and later.
- Red Hat Enterprise Linux 7.2 and later.
- Red Hat Enterprise Linux 8.0 and later.
- Red Hat Enterprise Linux 9.0 and later.
- Rocky Linux 8.5 and later.
- Rocky Linux 9.1.

- SberLinux 8.8 (Dykhtau).
- SberOS 3.2.0.
- SUSE Linux Enterprise Server 12.5 or later.
- SUSE Linux Enterprise Server 15 or later.
- Ubuntu® 20.04 LTS.
- Ubuntu 22.04 LTS.
- Ubuntu 24.04 LTS.
- ALT 8 SP Workstation (8.4).
- ALT 8 SP Server (8.4).
- ALT Education 10.1.
- ALT Workstation 10.1.
- ALT Server 10.1.
- ALT SP Workstation release 10.
- ALT SP Server release 10.
- Atlant, Alcyone build, version 2022.02.
- GosLinux 7.17.
- GosLinux 7.2.
- MSVSPHERE 9.2 ARM.
- MSVSPHERE 9.2 SERVER.
- RED OS® 7.3.
- RED OS 8.0.
- ROSA Cobalt 7.9.
- ROSA Chrome 12.
- SynthesisM Client 8.6.
- SynthesisM Server 8.6.

- 64-bit operating systems for the Arm architecture:
  - Astra Linux Special Edition RUSB.10152-02 (operational update 4.7).
  - CentOS Stream 9.

- EulerOS 2.0 SP10.
- SUSE Linux Enterprise Server 15.
- Ubuntu 22.04 LTS.
- ALT 8 SP Workstation (8.4).
- ALT 8 SP Server (8.4).
- ALT SP Workstation release 10.
- ALT SP Server release 10.
- RED OS 7.3.

Using Kaspersky Endpoint Security in Light Agent mode to protect virtual environments is not supported on operating systems for the Arm architecture.

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

Supported versions of Kaspersky Security Center

Kaspersky Endpoint Security is compatible with the following Kaspersky Security Center versions:

- Kaspersky Security Center 13.2. The MMC administration plug-in can be used to administer Kaspersky Endpoint Security via Administration Console.
- Kaspersky Security Center 14. Kaspersky Endpoint Security can be administered through Administration Console using the MMC administration plug-in and through Kaspersky Security Center Web Console using the web administration plug-in.
- Kaspersky Security Center 14.2 Windows. Kaspersky Endpoint Security can be administered through Administration Console using the MMC administration plug-in and through Kaspersky Security Center Web Console using the web administration plug-in.
- Kaspersky Security Center 14.2 Linux. The web administration plug-in can be used to administer Kaspersky Endpoint Security through Kaspersky Security Center Web Console.
- Kaspersky Security Center 15 Linux. The web administration plug-in can be used to administer Kaspersky Endpoint Security through Kaspersky Security Center Web Console.
- Kaspersky Security Center 15.1 Linux. The web administration plug-in can be used to administer Kaspersky Endpoint Security through Kaspersky Security Center Web Console.

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments (as part of Kaspersky Security for Virtualization Light Agent), we recommend to manage the application using one of the following versions of Kaspersky Security Center.

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Kaspersky Security Center Network Agent is required to manage Kaspersky Endpoint Security through Kaspersky Security Center.

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

If you are using application integration with the Kaspersky Endpoint Detection and Response (KATA) component, we recommend using the following versions of Kaspersky Security Center to manage the application:

- Kaspersky Security Center 14.2 Windows.
- Kaspersky Security Center 15 Linux.
- Kaspersky Security Center 15.1 Linux.

Supported versions of Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security is compatible with the following versions of Kaspersky Anti Targeted Attack Platform:

- Kaspersky Anti Targeted Attack Platform 5.1. Supported with limitations.
- Kaspersky Anti Targeted Attack Platform 6.0.
- Kaspersky Anti Targeted Attack Platform 6.1.

For more details about the Kaspersky Anti Targeted Attack Platform solution, please refer to the Kaspersky Anti Targeted Attack Platform Help.

What's new

Kaspersky Endpoint Security now boasts the following 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 working 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 parameters 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. If Kaspersky Endpoint Security is being used in Light Agent mode, integration with Kaspersky Symphony XDR is not supported.

- Now you can send information about all devices installed in client devices or connected to them (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.

- The list of supported operating systems has been updated.

Preparing to install Kaspersky Endpoint Security

General actions

Before starting installation of Kaspersky Endpoint Security, you need to perform the following actions:

- Check that your device meets the hardware and software requirements of the application.
- Be sure third-party anti-virus software is not installed on your device.
- Be sure that Kaspersky Endpoint Agent for Linux is not installed on your device. If Kaspersky Endpoint Agent for Linux is installed, during the installation process you will see a message about the need to manually remote it.
- Be sure that an interpreter for Perl version 5.10 or higher is installed on your device.
- On devices with operating systems that do not support fanotify technology, make sure that the following are installed:
  - 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.
- Install one of the following packages on your device depending on the operating system:
  - On devices running the SUSE Linux Enterprise Server 15 operating system, the insserv-compat package must be installed.
  - On devices running the Red Hat Enterprise Linux 8 or RED OS operating system, install the perl-Getopt-Long package.
  - On devices running the Red Hat Enterprise Linux or RED OS operating systems, install the perl-File-Copy package. This package is required for the initial application configuration script to work, but may be absent by default.
- 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, unblock 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).
- If your device uses a Linux kernel lower than 3.16, then in order for the Kaspersky Endpoint Detection and Response (KATA) Integration, you need to make sure the auditd service is not started and not installed.
- For the Firewall Management, Web Threat Protection and Network Threat Protection components to work, the iptables utility needs to be installed on your device.
- For the Kaspersky Endpoint Security administration plug-in to work, Microsoft® Visual C++® 2015 Redistributable Update 3 RC (see https://www.microsoft.com/en-us/download/details.aspx?id=52685) must be installed on the Administration Server.
- For the application to run correctly, make sure that the root account is the owner of the following directories and that only the owner has the right to write to them: /var, /var/opt, /var/opt/kaspersky, /var/log/kaspersky, /opt, /opt/kaspersky, /usr/bin, /usr/lib, /usr/lib64.

Additional actions before installing Kaspersky Endpoint Security in Light Agent mode

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments (as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent), you must perform the following additional actions before starting the installation of Kaspersky Endpoint Security:

- Make sure that the following packages are installed on the virtual machines that you want to protect, depending on the virtual infrastructure in which Kaspersky Hybrid Cloud Security for Virtualization Light Agent is deployed:
  - In a Microsoft Hyper-V infrastructure, the Integration Services package must be installed on the virtual machines.
  - In a VMware vSphere infrastructure, the VMware Tools package must be installed on the virtual machines.
  - In a XenServer infrastructure, XenTools must be installed on the virtual machines.
  - In a HUAWEI FusionSphere infrastructure, the HUAWEI Tools package must be installed on the virtual machines.
  - In an infrastructure based on KVM, OpenStack, VK Cloud, TIONIX Cloud Platform, Astra Linux, or Viola Virtualization Server, QEMU Guest Agent must be installed on virtual machines.
- 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. For more details about the solution components, please refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

Ports used for operation of the Light Agent

Port and protocol	Direction	Purpose and description
7271 TCP	From the Light Agent to the Integration Server.	For interaction between the Light Agent and the Integration Server.
8000 UDP	From the SVM to the Light Agent.	For transmitting information about available SVMs to Light Agents using a list of SVM addresses.
8000 UDP	From the Light Agent to SVMs.	For the Light Agent to receive information about the status of the SVM.
11111 TCP	From the Light Agent to SVMs.	For transmitting service requests (for example, to obtain license information) from the Light Agent to the Protection Server when the connection is unprotected.
11112 TCP	From the Light Agent to SVMs.	For transmitting service requests (for example, to obtain license information) from the Light Agent to the Protection Server when the connection is protected.
9876 TCP	From the Light Agent to SVMs.	For forwarding file scan requests from the Light Agent to the Protection Server when the connection is unprotected.
9877 TCP	From the Light Agent to SVMs.	For transmitting file scan requests from the Light Agent to the Protection Server when the connection is protected.
80 TCP	From the Light Agent to SVMs.	For updating databases and application modules of the solution on the Light Agent.

15000 UDP	From Kaspersky Security Center to SVMs.	For managing the Protection Server via Kaspersky Security Center.
15000 UDP	From Kaspersky Security Center to Light Agents.	For managing the Light Agent via Kaspersky Security Center.
13000 TCP	From the Light Agent to Kaspersky Security Center.	For managing the Light Agent via Kaspersky Security Center when the connection is protected.
14000 TCP	From the Light Agent to Kaspersky Security Center.	For managing Light Agent via Kaspersky Security Center when the connection is unprotected.

Installation and initial configuration of Kaspersky Endpoint Security

You need to prepare for installation before installing Kaspersky Endpoint Security.

The scenarios below describe how to install and perform initial configuration of Kaspersky Endpoint Security, how to install and configure Kaspersky Security Center Network Agent and how to install Kaspersky Endpoint Security administration plug-ins. The installation scenario depends on the mode in which you plan to use Kaspersky Endpoint Security.

Standard mode

If you plan to use Kaspersky Endpoint Security in Standard mode, the installation procedure involves the following steps:

1. **Installation and initial configuration of the Network Agent**

   If you plan to manage Kaspersky Endpoint Security using Kaspersky Security Center, install and configure Kaspersky Security Center Network Agent on the protected device.

2. **Installing the Kaspersky Endpoint Security administration plug-in**

   If you plan to manage Kaspersky Endpoint Security using Kaspersky Security Center, install the Kaspersky Endpoint Security administration plug-in. Depending on the console used to manage Kaspersky Security Center, the following administration plug-ins are used:

   - The Kaspersky Endpoint Security management web plug-in lets you manage the application using Kaspersky Security Center Cloud Console and Kaspersky Security Center Web Console. The web plug-in is installed on the device that has the Kaspersky Security Center Web Console installed.
   - The Kaspersky Endpoint Security MMC administration 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.

3. **Installing application packages and graphical user interface**

   Kaspersky Endpoint Security is distributed in the DEB and RPM packages. There are separate packages for the application and for the graphical user interface. Install Kaspersky Endpoint Security and, if necessary, the graphical user interface from packages in the appropriate format.

   You can perform installation in one of the following ways:

   - Using Kaspersky Security Center.
   - Using the command line.

4. **Initial configuration of Kaspersky Endpoint Security**

   The initial configuration must be performed to enable the protection of the client device.

   If you installed Kaspersky Endpoint Security using Kaspersky Security Center, after the installation is complete, go through the Getting started procedure.

   If you installed Kaspersky Endpoint Security using the command line, run the initial configuration script or perform the initial configuration in automatic mode after installation is completed.

Light Agent mode

Using Kaspersky Endpoint Security in Light Agent mode to protect virtual environments is not supported on operating systems based on the Arm architecture.

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments, the installation procedure involves the following steps:

1. **Installation and initial configuration of the Network Agent**

   Install and configure Kaspersky Security Center Agent on virtual machines and virtual machine templates.

   If you are installing Network Agent on a template that will be used to create temporary virtual machines, it is recommended to configure settings that allow you to optimize performance on temporary virtual machines. For more details about installing on a virtual machine template, refer to the Help for Kaspersky Security for Virtualization Light Agent.

2. **Installing the Kaspersky Endpoint Security administration plug-in**

   Install a Kaspersky Endpoint Security administration plug-in. Depending on the console used to manage Kaspersky Security Center, the following administration plug-ins are used:

   - The Kaspersky Endpoint Security management web plug-in lets you manage the application using Kaspersky Security Center Cloud Console and Kaspersky Security Center Web Console. The web plug-in is installed on the device that has Kaspersky Security Center Web Console installed.
   - The Kaspersky Endpoint Security MMC administration 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.

3. **Installation of application packages and initial configuration of Kaspersky Endpoint Security**

   Kaspersky Endpoint Security is distributed in the DEB and RPM packages. Install Kaspersky Endpoint Security from a package of the required format. There are separate packages for the application and for the graphical user interface.

   The graphical user interface is not supported if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments.

   You can install the application in one of the following ways:

   - Using Kaspersky Security Center.

     Before starting the installation, you must perform the initial configuration of the application in one of the following ways:

     - In the properties of the installation package on the **Settings** tab (this method is available only in Kaspersky Security Center Web Console).
     - Using the configuration file, which is included in the installation package.

     You must select the Light Agent mode (`KSVLA_MODE=yes` in the configuration file). If you are installing Kaspersky Endpoint Security on a template from which temporary virtual machines will be created, we recommend to also enable VDI protection mode to optimize the performance of the application on temporary virtual machines (`VDI_MODE=yes` in the configuration file).

   - Using the command line. If installation is performed using the command line, the application usage mode is selected during initial configuration.

4. **Initial configuration of Kaspersky Endpoint Security**

The initial configuration must be performed to enable the protection of the client device.

If you installed Kaspersky Endpoint Security using Kaspersky Security Center, after the installation is complete, go through the Getting started procedure.

If you installed Kaspersky Endpoint Security using the command line, run the initial configuration script or perform the initial configuration in automatic mode after installation is completed. During initial configuration, select Light Agent mode in one of the following ways:

- Enter `yes` in the `Specifying the application usage` step of the initial configuration script.
- Specify the `KSVLA_MODE=yes` setting in the initial setup configuration file.

If you install Kaspersky Endpoint Security on a template that will be used to create temporary virtual machines, it is recommended to also configure the setting for optimizing the operation on temporary virtual machines. For more details about installing on a virtual machine template, refer to the Help for Kaspersky Security for Virtualization Light Agent.

The installation and initial configuration of Kaspersky Security Center Network Agent

Network Agent must be installed in order to manage Kaspersky Endpoint Security via Kaspersky Security Center.

Network Agent facilitates the client device's connection with the Kaspersky Security Center Administration Server. It must be installed on every client device that will be connected to Kaspersky Security Center, the centralized remote management system.

You can perform the installation and initial configuration of Network Agent:

- remotely from the administrator's workstation using the Kaspersky Security Center Web Console or the Administration Console;
- using the command line.

Installing Network Agent using Kaspersky Security Center

Before starting remote installation of Network Agent using Kaspersky Security Center, you must prepare the device for remote installation (see the Kaspersky Security Center Help system, section "Preparing a device running Linux and installing Network Agent remotely on a device running Linux").

The Network Agent installation package is used for remote installation. You can download the files necessary for creating a Network Agent installation package from the Kaspersky website in the **Kaspersky Security Center** section.

To install Network Agent remotely:

1. Create the Network Agent installation package.

   During creation of the installation package, you must accept the conditions of the End User License Agreement for Network Agent. You can read the text of the End User License Agreement in the license.txt document from the Network Agent distribution kit.

   In the installation package settings, specify the address of the Administration Server to which Network Agent should connect, as well as the connection port.

2. Install Network Agent using the remote installation task.

For more details on how to install Network Agent, refer to the Kaspersky Security Center Help system.

Installing Network Agent using the command line

You can install Network Agent using the command line in one of the following ways:

- Run the installation and initial configuration in silent mode with an answer file. An answer file is a text file that contains a custom set of settings for the installation and initial configuration of Network Agent.
- Install Network Agent from an RPM or DEB package in accordance with the type of package manager, then perform initial configuration of Network Agent using a script in interactive mode. The script is run with the following command:
  - for a 32-bit operating system:

    ```
    # /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
    ```

  - for a 64-bit operating system:

    ```
    # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
    ```

The Network Agent installation must be started with root privileges.

To install Network Agent in silent mode:

1. Create an answer file. In the answer file, enter a list of Network Agent installation and initial configuration settings in the format `<setting>=<value>`, with each setting on a separate line.

   To use an answer file correctly, you must include the following required settings:

   - KLNAGENT_SERVER: fully qualified domain name (FQDN) or IP address of the Administration Server.
   - KLNAGENT_AUTOINSTALL: this setting determines whether installation in silent mode is enabled. Specify `1`.
   - EULA_ACCEPTED: consent to the conditions of the End User License Agreement for Network Agent. You must accept the terms of the End User License Agreement to continue the installation. You can read the text of the End User License Agreement in the license.txt document from the Network Agent distribution kit. If you understand and accept the conditions of the End User License Agreement, specify `1`.

   You can also add other settings for the installation and initial configuration of Network Agent. For a full list of possible settings, refer to the Kaspersky Security Center Help system (section "Installing Network Agent for Linux in silent mode (with an answer file)").

2. Set the value of the KLAUTOANSWERS environment variable by entering the full name of the answer file (including the path), as per the following example:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

3. Install Network Agent:

   - To install Network Agent from an RPM package to a 32-bit operating system, execute the following command:

     ```
     # rpm -i klnagent-<build number>.i386.rpm
     ```

- To install Network Agent from an RPM package to a 64-bit operating system, execute the following command:

  ```
  # rpm -i klnagent64-<build number>.x86_64.rpm
  ```

- To install Network Agent from an RPM package on a 64-bit operating system for the Arm architecture, execute the following command:

  ```
  # rpm -i klnagent64-<build number>.aarch64.rpm
  ```

- To install Network Agent from a DEB package to a 32-bit operating system, execute the following command:

  ```
  # apt-get install ./klnagent_<build number>_i386.deb
  ```

- To install Network Agent from a DEB package to a 64-bit operating system, execute the following command:

  ```
  # apt-get install ./klnagent64_<build number>_amd64.deb
  ```

- To install Network Agent from a DEB package on a 64-bit operating system for the Arm architecture, execute the following command:

  ```
  # apt-get install ./klnagent64_<build number>_arm64.deb
  ```

Installing Kaspersky Endpoint Security administration plug-ins

The following Kaspersky Endpoint Security administration plug-ins are used to manage Kaspersky Endpoint Security using Kaspersky Security Center:

- The Kaspersky Endpoint Security administration web plug-in lets you manage the application using Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console.

- The Kaspersky Endpoint Security MMC administration plug-in lets you manage the application using Kaspersky Security Center Administration Console.

You can install administration plug-ins for different versions of Kaspersky Endpoint Security simultaneously. 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.

Installing Kaspersky Endpoint Security web plug-in

The Kaspersky Endpoint Security administration web plug-in must be installed on the client 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.

You can install the web plug-in as follows:

- Using the Initial Configuration Wizard for Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console automatically prompts you to run the Initial Configuration 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 → Initial Configuration Wizard**). The Initial Configuration Wizard can also check if the installed web plug-ins are up to date and download the necessary updates. For more information on the Initial Configuration Wizard for Kaspersky Security Center Web Console, please refer to Kaspersky Security Center Help section.

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

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

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. Start the installation of the Kaspersky Endpoint Security web plug-in by one of the following ways:

   - Installation from the list of Kaspersky web plug-ins:

     a. Click **Add**.

     A list of all available Kaspersky Web plug-ins opens. The list is updated automatically after new versions of web plug-ins are released.

     b. Find the **Kaspersky Endpoint Security <version number> for Linux** web plug-in in the list and click its name.

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

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

   - Installation of the web plug-in from an external source (the archives required for installing the web plug-ins are included in the distribution kit):

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

     b. In the window that opens, specify the path to the ZIP archive with the distribution kit for the web plug-in and the path to the signed file in TXT format. This file is in the archive with the web plug-in.

     c. Click **Add**.

     d. 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.

Installing Kaspersky Endpoint Security MMC plug-in

The Kaspersky Endpoint Security MMC administration plug-in must be installed on the same client device where the Kaspersky Security Center Administration Console is installed.

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

To install the MMC plugin,

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

The file is included in the Kaspersky Endpoint Security distribution kit.

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

To view a list of installed MMC administration 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:
   - using the **Properties** item in the **Administration Server <server name>** node context menu;
   - by clicking the **Administration Server properties** link located 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 administration plug-ins** section.

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

Installing and initially configuring the application using Kaspersky Security Center

You can install Kaspersky Endpoint Security on a client device remotely from the administrator's workstation using the Kaspersky Security Center Web Console or the Administration Console.

For the remote installation, Kaspersky Endpoint Security installation package is used. Kaspersky Endpoint Security installation package is common for all supported operating systems and processor architecture types. You can create the installation package using the Kaspersky Security Center Web Console or the Administration Console.

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments (as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent), you need to perform the initial configuration of the application in installation package properties (this method is available only in the Web Console) or in the autoinstall.ini configuration file which is included in the installation package.

You can deploy Kaspersky Endpoint Security on the devices in the corporate network in several ways.

Kaspersky Security Center Web Console supports the following main deployment methods:

- Installing the application using the Protection Deployment Wizard.
- Installing the application using the remote installation task.

The Kaspersky Security Center Administration Console supports the following main deployment methods:

- Installing the application using the Remote Installation Wizard.
- Installing the application using the remote installation task.

For a description of the deployment procedures, see the Kaspersky Security Center Help.

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

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, then activation of the application during installation and automatic license key distribution are not supported. If Kaspersky Endpoint Security receives information about the license from the Protection Server after connecting to the SVM; there is no need to activate Kaspersky Endpoint Security separately.

After installation of the application using Kaspersky Security Center is complete, you must prepare the application for operation.

To use Kaspersky Security Center to manage Kaspersky Endpoint Security installed on client devices, you need to put these devices in administration groups. Before starting Kaspersky Endpoint Security installation, you can create Kaspersky Security Center administration groups to which you want to move the devices with Kaspersky Endpoint Security installed, and configure the rules to automatically move the devices to these administration groups. If rules for moving devices to the administration groups are not configured, Kaspersky Security Center moves all the devices that have the Administration Agent installed and are connected to Administration Server to the **Unassigned devices** list. In this case, you need to manually move computers to the administration groups (refer to the Kaspersky Security Center Help for details).

Creating an installation package in the Web Console

In Kaspersky Security Center Web Console, you can create an installation package in one of the following ways:

- From an archive file that you have prepared previously.
- From a distribution kit hosted on Kaspersky servers.

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments, you must perform the initial configuration of the application in the properties of the created installation package on the **Settings** tab. You can also perform the initial configuration of the application using the configuration file that is included in the installation package.

To prepare an archive for creating an installation package:

1. Download the kesl.zip archive from the application download page. It is located in the **Kaspersky Endpoint Security for Linux** (**Additional distribution -> Files for Product remote installation**).

2. Unpack the kesl.zip archive to a folder accessible to Kaspersky Security Center Administration Server. Place the distribution files, that correspond to the type of operating system where you want to install the application and the type of its package manager, to the same folder:

   - To install Kaspersky Endpoint Security:
     - kesl-12.1.0-<build number>.i386.rpm (for 32-bit operating systems with rpm)
     - kesl_12.1.0-<build number>_i386.deb (for 32-bit operating systems with dpkg)
     - kesl-12.1.0-<build number>.x86_64.rpm (for 64-bit operating systems with rpm)
     - kesl_12.1.0-<build number>_amd64.deb (for 64-bit operating systems with dpkg)
     - kesl-12.1.0-<build number>.aarch64.rpm (for 64-bit operating systems with rpm for the Arm architecture)
     - kesl_12.1.0-<build number>_arm64.deb (for 64-bit operating systems with dpkg for the Arm architecture)
   - to install the GUI:
     - kesl-gui-12.1.0-<build number>.i386.rpm (for 32-bit operating systems with rpm)
     - kesl-gui_12.1.0-<build number>_i386.deb (for 32-bit operating systems with dpkg)
     - kesl-gui-12.1.0-<build number>.x86_64.rpm (for 64-bit operating systems with rpm)
     - kesl-gui_12.1.0-<build number>_amd64.deb (for 64-bit operating systems with dpkg)
     - kesl-gui-12.1.0-<build number>.aarch64.rpm (for 64-bit operating systems with rpm for the Arm architecture)
     - kesl-gui_12.1.0-<build number>_arm64.deb (for 64-bit operating systems with dpkg for the Arm architecture)

     If you do not want to install a graphical user interface, do not put these files into the folder; this will make the installation package smaller.

     If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the graphical user interface is not supported.

   Note that If you are not planning to use the graphical user interface, you need to set `USE_GUI=No` in the properties of the created installation package or in the autoinstall.ini configuration file. Otherwise, the installation will fail.

   If you want to use the created installation package to install the application on several types of operating systems or package managers, place the files for all the required types of operating systems and package managers in the folder.

3. If you want to perform 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 where you unpacked the kesl.zip archive.

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments, you need to set `KSVLA_MODE=yes` in the autoinstall.ini configuration file.

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

4. If you plan to use Kaspersky Endpoint Security in Standard mode and want to use previously downloaded databases, place the prepared archives with databases for all required operating system types in the folder. Open the autoinstall.ini configuration file and specify `UPDATE_EXECUTE=no`. The autoinstall.ini file is located in the folder where you unpacked the kesl.zip archive.

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

To create an installation package for Kaspersky Endpoint Security in Kaspersky Security Center Web Console:

1. 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.

2. Click **Add**.

   The wizard for creating an installation package will start. Follow the instructions of the Wizard.

3. On the first page of the wizard, select the method for creating 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. You need to select this option if you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments.
   - **Create installation package for a Kaspersky application**. The installation package will be created from a distribution package located on Kaspersky servers.

   Kaspersky Security Center Cloud Console does not allow creation of installation packages from a file.

4. Depending on the selected 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. During creation of the installation package, accept the terms of the End User License Agreement and Privacy Policy. When prompted by the Wizard, read the License Agreement between you and Kaspersky and the Privacy Policy that describes the processing and transmission of data. To continue creating the installation package, you must confirm that you have fully read and accept the terms of the License Agreement and the Privacy Policy.

The installation package will be created and added to the list of installation packages. Using the installation package, you can install the application on devices in the corporate network or update the application version.

You can perform the initial configuration of the application in the properties of the installation package, on the **Settings** tab (see the table below).

An installation package for Kaspersky Endpoint Security cannot be configured in Kaspersky Security Center Web Console versions lower than 14.2. Use the autoinstall.ini configuration file to configure settings.

Installation package settings

Section	Description
Specify the locale.	Select this check box to specify the locale used during the application operation. The locale in the format specified by RFC 3066. If this setting is not specified, the default locale is used.
Activate the application	Select the check box to activate the application. You can also activate the application after installation. This setting applies only if the application is used in Standard mode.
Select the update source.	Specify the update source: • **Kaspersky update servers**. • **Kaspersky Security Center**. • **Other source in the local or global network**. This setting applies only if the application is used in Standard mode.
Run the database update task after installation.	Select this check box to run the Update task after the application is installed. This setting applies only if the application is used in Standard mode.
Specify the proxy server settings.	Select this check box to specify the address of the proxy server used to connect to the Internet. This setting applies only if the application is used in Standard mode.
Install kernel source	Select this check box to automatically start of kernel module compilation.

Use the graphical user interface.	Select this check box to enable the use of the graphical user interface. This setting applies only if the application is used in Standard mode.
Specify a user with the admin role.	Select the check box to specify the user to be assigned the administrator (admin) role.
Configure SELinux automatically.	Select the check box to automatically configure SELinux to work with Kaspersky Endpoint Security.
Remove users from privileged groups	Select this check box to remove users from the 'kesladmin' and 'keslaudit' privileged groups before installing the application. 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 when the application is started for the first time after installation.	Select this check box to start the application with protection components and scan tasks disabled after installation. An installation with protection components disabled can be convenient, for example, in order 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.
Use the application in Light Agent mode	Select the check box if you want to use the application in Light Agent mode to protect virtual environments (as part of Kaspersky Security for Virtualization Light Agent). If this check box is cleared, the application is used in Standard mode.
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. The setting is applied only if the application is used in Light Agent mode.
The protected virtual machine is used as a server.	Select this check box if the virtual machine on which you are installing the application is used in the virtual infrastructure as a server. The setting is applied only if the application is used in Light Agent mode.

Creating an installation package in the Administration Console

Before creating an installation package for Kaspersky Endpoint Security, you need to prepare the files to be included in the package.

To prepare files for creating an installation package:

1. Download the kesl.zip archive from the application download page. It is located in the **Kaspersky Endpoint Security for Linux** (**Additional distribution -> Files for Product remote installation**).

2. Unpack the kesl.zip archive to a folder accessible to Kaspersky Security Center Administration Server. Place the distribution files, that correspond to the type of operating system where you want to install the application and the type of its package manager, to the same folder:

   - To install Kaspersky Endpoint Security:
     - kesl-12.1.0-<build number>.i386.rpm (for 32-bit operating systems with rpm)
     - kesl_12.1.0-<build number>_i386.deb (for 32-bit operating systems with dpkg)
     - kesl-12.1.0-<build number>.x86_64.rpm (for 64-bit operating systems with rpm)
     - kesl_12.1.0-<build number>_amd64.deb (for 64-bit operating systems with dpkg)
     - kesl-12.1.0-<build number>.aarch64.rpm (for 64-bit operating systems with rpm for the Arm architecture)
     - kesl_12.1.0-<build number>_arm64.deb (for 64-bit operating systems with dpkg for the Arm architecture)
   - to install the GUI:
     - kesl-gui-12.1.0-<build number>.i386.rpm (for 32-bit operating systems with rpm)
     - kesl-gui_12.1.0-<build number>_i386.deb (for 32-bit operating systems with dpkg)
     - kesl-gui-12.1.0-<build number>.x86_64.rpm (for 64-bit operating systems with rpm)
     - kesl-gui_12.1.0-<build number>_amd64.deb (for 64-bit operating systems with dpkg)
     - kesl-gui-12.1.0-<build number>.aarch64.rpm (for 64-bit operating systems with rpm for the Arm architecture)
     - kesl-gui_12.1.0-<build number>_arm64.deb (for 64-bit operating systems with dpkg for the Arm architecture)

     If you do not want to install a graphical user interface, do not put these files into the folder; this will make the installation package smaller.

     If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the graphical user interface is not supported.

Note that If you are not planning to use the graphical user interface, you need to set `USE_GUI=No` in the properties of the created installation package or in the autoinstall.ini configuration file. Otherwise, the installation will fail.

If you want to use the created installation package to install the application on several types of operating systems or package managers, place the files for all the required types of operating systems and package managers in the folder.

3. If you want to perform 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 where you unpacked the kesl.zip archive.

   If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments, you need to set `KSVLA_MODE=yes` in the autoinstall.ini configuration file.

4. If you plan to use Kaspersky Endpoint Security in Standard mode and want to use previously downloaded databases, place the prepared archives with databases for all required operating system types in the folder. Open the autoinstall.ini configuration file and specify `UPDATE_EXECUTE=no`. The autoinstall.ini file is located in the folder where you unpacked the kesl.zip archive.

To create an installation package for Kaspersky Endpoint Security in the Administration Console of Kaspersky Security Center:

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. In the wizard window that opens, click the **Create an installation package for Kaspersky application** button.
4. Enter the name of the new installation package and proceed to the next step.
5. Select Kaspersky Endpoint Security distribution package. To do this, open a standard browsing window using the **Browse** button and specify the path to the kesl.kud file. The file is located in the folder where you unpacked the kesl.zip archive.

   The application name is displayed in the window.

   Proceed to the next step.
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 creating the installation package, you must confirm that you have fully read and accept the terms of the License Agreement and the Privacy Policy. To confirm, in the window that opens, select both check boxes.

   Proceed to the next step.
7. The wizard downloads the files required to install the application to Kaspersky Security Center Administration Server. Wait for the download to finish.
8. Complete the wizard.

The created installation package is located in the tree of the Administration Console of Kaspersky Security Center in the **Additional** → **Remote installation** → **Installation packages** folder. You can use the same installation package many times.

Preparing an archive with application databases in order to create an installation package with integrated databases

In some cases, you may need to create a remote installation package with pre-downloaded application databases. For example, if you install the application on a device running the Astra Linux Special Edition operating system or want to install the application immediately with prepared current databases (so as to avoid separately updating the databases later).

To create an installation package with integrated databases for installing the application:

1. Install and perform the initial configuration of Kaspersky Endpoint Security on the device using the command line or using Kaspersky Security Center.

2. Update the application databases. You can update the databases during the initial configuration of the application or after installation by running a task of an Update type in the command line or an *Update* task in the Kaspersky Security Center Administration Console or the Kaspersky Security Center Web Console.

3. Copy the contents of the /var/opt/kaspersky/kesl/private/updates/ directory to one of the following subdirectories, depending on the architecture of the operating system for which you are creating the installation package with integrated databases: /i386/, /x86_64/, or /arm64/.

4. Place the directories with the databases into a kesl-bases.tgz archive, preserving the structure of nested directories. You can place only one subdirectory with databases for the required architecture of the operating system in the archive, or if you plan to create an installation package for installation on several operating systems with different architectures, you can place all the subdirectories with databases (/i386/, /x86_64/, or /arm64/) into a single archive for different architectures.

5. You can use the created archive with application databases when creating an installation package in the Kaspersky Security Center Administration Console or Kaspersky Security Center Web Console.

Autoinstall.ini configuration file settings

In the autoinstall.ini configuration file, you can specify the settings shown in the table below. The set of applicable settings depends on the application usage mode.

Autoinstall.ini configuration file settings

Setting	Description	Values
KSVLA_MODE	Kaspersky Endpoint Security usage mode.	`yes` - Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments (as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent). `no` (default value) – Kaspersky Endpoint Security is used in Standard mode.
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.	`yes` (default value) – 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	`yes` – enable VDI protection mode. This is recommended if you are installing

	performance on temporary virtual machines. The setting is applied only if the application is used in Light Agent mode.	Kaspersky Endpoint Security on a virtual machine template that will be used to create temporary virtual machines. `no` (default value) – do not enable VDI protection mode.
EULA_AGREED	Required setting. Acceptance of the terms of the End User License Agreement.	`yes` (default value) – accept the terms of the End User License Agreement to continue the application installation procedure. `no` – do not accept 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 value) – accept the terms of the Privacy Policy to continue the application installation procedure. `no`: do not accept the Privacy Policy. The application installation will be terminated.
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.	`yes` – accept the terms of the Kaspersky Security Network Statement and enable the use of KSN. `no` – (default value) do not accept the Kaspersky Security Network Statement. 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.
GROUP_CLEAN	Required setting. Removing users from the kesladmin and keslaudit privileged groups.	`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` - Do not remove users from the privileged groups.
LOCALE	Optional setting. The locale used for the application events sent to Kaspersky Security Center.	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 fails to determine the operating system localization language or the operating system localization is not supported, the default value will be used – `en_US.utf8`.

		The locale of the graphical interface and the application command line depends on the value of the `LANG` environment variable. If the locale that is not supported by Kaspersky Endpoint Security is specified as the value of the `LANG` environment variable, the graphical interface and the command line are displayed in English.
INSTALL_LICENSE	Activation code or key file. This setting applies only if the application is used in Standard mode.	
UPDATER_SOURCE	Update source. This setting applies only if the application is used in Standard mode.	`SCServer` – use the Kaspersky Security Center Administration Server as the update source. `KLServers` – use Kaspersky servers as the update source. This value is used by default. Update source address
PROXY_SERVER	Address of the proxy server used to connect to the Internet. This setting applies only if the application is used in Standard mode.	Proxy server address
UPDATE_EXECUTE	Start application database update task during setup. This setting applies only if the application is used in Standard mode.	`yes` (default value) – start the update task. `no` – do not start update task.
KERNEL_SRCS_INSTALL	Automatic start of kernel module compilation.	`yes` (default value) — compile the kernel module. `no` – do not compile kernel module.
USE_GUI	Use of the graphical user interface. This setting applies only if the application is used in Standard mode.	`yes` – Enable use of the graphical user interface. `no` (default value) – Disable the use of the graphical user interface.

ADMIN_USER	A user assigned the administrator role (admin).	No
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 automatically configure SELinux to work with Kaspersky Endpoint Security.
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.
DISABLE_FILEAV_ACTIONS	Disables the disinfection and file deletion functions for application components after its installation. If the disinfection and file deletion functions are disabled and a threat is detected, the application does not attempt to disinfect or delete the files in which a threat was detected, but only informs the user about a threat detected in files. After installing the application, you can enable the file disinfection and deletion functionality using the `DisableFileAvActions` parameter in the kesl.ini configuration file.	`yes`: disables the disinfection and file deletion functions when the application is started after the installation. `no` (default value): does not disable the disinfection and file deletion functions when the application is started after the installation.

If you want to change the settings in the autoinstall.ini configuration file, specify the values of settings in the following format: <setting_name>=<setting_value> (the application does not process spaces between the name of a setting and its value).

Getting started using Kaspersky Security Center

After deploying Kaspersky Endpoint Security through Kaspersky Security Center, you must prepare the application for operation. The actions to be performed depend on the mode in which you plan to use Kaspersky Endpoint Security.

Standard mode

If you plan to use Kaspersky Endpoint Security in Standard mode, after deploying the application, you need to do the following:

- Activate the application. You can create and execute an activation task using the Administration Console or Kaspersky Security Center Web Console, as well as distribute the license key to the devices from the Kaspersky Security Center key storage.
- Update application databases and modules using the Administration Console or Kaspersky Security Center Web Console. You can use the *Update* task, which is created automatically by the initial configuration wizard of Kaspersky Security Center after installing the MMC administration plug-in or the Kaspersky Endpoint Security web administration plug-in.
- Configure a policy for centralized management of the application using Kaspersky Security Center Administration Console or Web Console. You can use a policy that is created automatically by the initial configuration wizard of Kaspersky Security Center after installing the MMC administration plug-in or the Kaspersky Endpoint Security web administration plug-in.

  You can also configure the application management tasks using the Administration Console or the Web Console.

Light Agent mode

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments, after deploying the application, perform the following actions:

1. Configure SVM detection settings for Light Agents. To do this, you need to create and configure a policy for centralized application management on client devices. You can use the Administration Console or the Web Console to work with policies.

   You need to configure the following settings in the policy properties:

   - Settings for connecting Light Agents to the Integration Server.
   - Settings for connecting Light Agents to SVMs.

2. Make sure that a connection is established between Light Agents and the SVMs and the Integration Server.

   You can get information about the connection by using Kaspersky Endpoint Security commands on the protected virtual machine:

   - You can view information about connecting to SVMs using the `kesl-control [-V] --svm-info` command.
   - You can view information about connecting to the Integration Server using the `kesl-control [-V] --viis-info` command.

3. Make sure that Kaspersky Endpoint Security used as a Light Agent receives information about the license under which Kaspersky Hybrid Cloud Security for Virtualization Light Agent is activated.

After activating the solution on SVMs and connecting Light Agents to the SVMs, the Protection Server component sends license information to Light Agents. Information about the license used by Kaspersky Endpoint Security as part of the solution can be viewed on the protected virtual machine using the `kesl-control -L --query` command.

4. Make sure that database updates required for Light Agent to operate are installed on the protected virtual machines.

   Databases on protected virtual machines are updated using a special *Update* task, in which a folder on the SVM is specified as the update source. The update task starts automatically.

   You can check how up-to-date the databases are on a protected virtual machine with Light Agent by using the `kesl-control --app-info` command.

   You can also configure the application management tasks using the Administration Console or the Web Console.

Activating the application using Kaspersky Security Center

Activation is the process of activating a license that allows you to use a fully functional version of the application until the license expires.

If you plan to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments, you do not need to activate the application after installation. You activate Kaspersky Hybrid Cloud Security for Virtualization Light Agent on the Protection Server (a component of Kaspersky Hybrid Cloud Security for Virtualization Light Agent) by adding a license key to the SVM. For more details, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

The process of activating Kaspersky Endpoint Security involves adding an application license key.

If you are using the application under a license that does not include the Kaspersky Endpoint Detection and Response Optimum functionality, then to activate this functionality, you need to add an additional Kaspersky Endpoint Detection and Response Optimum Add-on license key ("EDR Optimum key").

You can add license keys to the application through Kaspersky Security Center in the following ways:

- Using the Add key task.

  This method allows you to add a license key to a specific device or the devices included in an administration group. You can create and run an Add key task using Kaspersky Security Center Web Console or the Administration Console.

- By distributing a license key stored on Kaspersky Security Center Administration Server to the client devices.

  This method lets you automatically add a key to the client devices that are already connected to Kaspersky Security Center, and to new client devices. To use this method, first add the key to the key storage on Kaspersky Security Center Administration Server.

- By adding the key to the Kaspersky Endpoint Security installation package.

  This method allows adding a key in the properties of the installation package when deploying Kaspersky Endpoint Security. The application will be activated automatically after installation.

You can use Kaspersky Security Center Administration Console or Kaspersky Security Center Web Console to create tasks for adding a key to the application, adding a key to the key storage, and distributing the key to the client devices.

Activation using Kaspersky Security Center Web Console

Before creating an Add key task or distributing a key, add the key to Kaspersky Security Center Administration Server key storage.

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 **Add**.
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 the file with the key extension.
5. Click **Close**.

The added key will appear in the list of keys.

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 **Assets (Devices)** → **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 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**.
   The **Kaspersky Security Center key storage** window opens.
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 required key cannot be found in the key storage, click the **Add Key** button.

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 the 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. Complete the wizard.

   A new task will be displayed in the list of tasks.
9. Select the check box next to the task. Click the **Start** button.

In the properties of the *Add Key* task, you can add a *reserve key* to the device. The reserve key becomes active when the license associated with the active key expires or when the active key is deleted. Availability of a reserve key allows you to avoid application functionality limitation when your license expires.

If you are adding a reserve key but no active key has been added to the application yet, the task ends with an error.

To add a key to the application using the Web Console by distributing a key stored on the Administration Server to the 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 **Save**.

   The license key is automatically distributed to the appropriate client devices. 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.

You can control license usage using Kaspersky Security Center Web Console in the following ways:

- View the License key usage report (**Monitoring & Reporting** → **Reports**).
- View the statuses of the managed devices (**Assets (Devices)** → **Managed devices**). If the application is not activated, the device will have the status and the **Protection disabled** status description.

- View the key properties (**Operations** → **Kaspersky licenses**).

Special considerations for the activation process in Kaspersky Security Center Cloud Console

A trial version is provided for the Kaspersky Security Center Cloud Console. The *trial version* is a special version of Kaspersky Security Center Cloud Console designed to familiarize a user with the features of the application. In this version, 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 Kaspersky Security Center Cloud Console expires. For detailed information about Kaspersky Security Center Cloud Console, please refer to the Kaspersky Security Center Cloud Console documentation.

The trial version of Kaspersky Security Center Cloud Console does not allow you to subsequently switch to a commercial version. Any trial workspace will be automatically deleted with all its contents after the 30-day period expires.

Installing and initially configuring the application using the command line

You can perform the following actions when installing the application using the command line:

- Install the application with the graphical user interface.

  If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments (as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent), the graphical user interface is not supported. You need to install only the application package without the graphical user interface.

- Install the application without the graphical user interface.
- Install the graphical user interface on the device where the application is installed.

  It is not possible to install the graphical user interface on a device on which the application is not installed.

If the version of the apt package manager is lower than 1.1.X, use the dpkg/rpm package manager (depending on the operating system) for installation.

After the installation of the application is complete, perform the initial configuration of the application interactively or automatically.

Installing the application using the command line

Installing the application without the graphical user interface

To install Kaspersky Endpoint Security from an RPM package on a 32-bit operating system, execute the following command:

```
# rpm -i kesl-12.1.0-<build number>.i386.rpm
```

To install Kaspersky Endpoint Security from an RPM package on a 64-bit operating system, execute the following command:

```
# rpm -i kesl-12.1.0-<build number>.x86_64.rpm
```

To install Kaspersky Endpoint Security from an RPM package on a 64-bit operating system for the Arm architecture, execute the following command:

```
# rpm -i kesl-12.1.0-<build number>.aarch64.rpm
```

To install Kaspersky Endpoint Security from a DEB package on a 32-bit operating system, execute the following command:

```
# apt-get install ./kesl_12.1.0-<build number>_i386.deb
```

To install Kaspersky Endpoint Security from a DEB package on a 64-bit operating system, execute the following command:

```
# apt-get install ./kesl_12.1.0-<build number>_amd64.deb
```

To install Kaspersky Endpoint Security from a DEB package on a 64-bit operating system for the Arm architecture, execute the following command:

```
# apt-get install ./kesl_12.1.0-<build number>_arm64.deb
```

Graphical user interface installation

To install the graphical user interface from the RPM package to a 32-bit operating system, execute the following command:

```
# rpm -i kesl-gui-12.1.0-<build number>.i386.rpm
```

To install the graphical user interface from the RPM package to a 64-bit operating system, execute the following command:

```
# rpm -i kesl-gui-12.1.0-<build number>.x86_64.rpm
```

To install the graphical user interface from an RPM package on a 64-bit operating system for the Arm architecture, execute the following command:

```
# rpm -i kesl-gui-12.1.0-<build number>.aarch64.rpm
```

To install the graphical user interface from the DEB package to a 32-bit operating system, execute the following command:

```
# apt-get install ./kesl-gui_12.1.0-<build number>_i386.deb
```

To install the graphical user interface from the DEB package to a 64-bit operating system, execute the following command:

```
# apt-get install ./kesl-gui_12.1.0-<build number>_amd64.deb
```

To install the graphical user interface from a DEB package on a 64-bit operating system for the Arm architecture, execute the following command:

```
# apt-get install ./kesl-gui_12.1.0-<build number>_arm64.deb
```

Initial configuration of the application in interactive mode

After installing Kaspersky Endpoint Security using the command line, perform the initial application setup by running the initial configuration script. The initial configuration script is included in the Kaspersky Endpoint Security distribution kit.

Performing the initial setup after installing the application using the command line is required to enable the protection of the client device.

To run Kaspersky Endpoint Security initial configuration script, execute the following command:

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

The initial configuration script must be run with the root privileges after the installation of Kaspersky Endpoint Security package is finished. The script requests the values of Kaspersky Endpoint Security settings step-by-step. Script execution completion and the console release indicate that the initial application setup is completed.

To check the return code, execute the following command:

```
echo $?
```

If the command returns code 0, the initial application setup is finished successfully.

Selecting the application usage mode

At this step, select the Kaspersky Endpoint Security usage mode:

- Enter `yes` if you want to use Kaspersky Endpoint Security in Light Agent mode to protect virtual environments.
- Enter `no` if you want to use Kaspersky Endpoint Security in Standard mode.

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

Defining the role of the virtual machine

This step is displayed only if at the first step you selected to use Kaspersky Endpoint Security in Light Agent mode for protecting virtual environments.

At this step, 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.

Enabling VDI protection mode

This step is displayed only if at the first step you selected to use Kaspersky Endpoint Security in Light Agent mode for protecting virtual environments.

At this step, you can enable VDI protection mode. This 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.

Selecting the locale

At this step, the application displays the list of supported locale identifiers in RFC 3066 format.

Specify the locale in the format as identified in this list. This locale will be used for application events sent to Kaspersky Security Center, as well as for the texts of the License Agreement, Privacy Policy, and Kaspersky Security Network Statement.

The locale of the graphical interface and the application command line depends on the value of the `LANG` environment variable. If the locale that is not supported by Kaspersky Endpoint Security is specified as the value of the `LANG` environment variable, the graphical interface and the command line are displayed in English.

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 handling and transmission of data.

Accepting the End User License Agreement

At this step, you must either accept or decline the terms of 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 do not accept the terms of the End User License Agreement, the application terminates Kaspersky Endpoint Security setup process.

Accepting the Privacy Policy

At this step, you must either accept or decline the terms of 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 do not accept the terms of the Privacy Policy, the application terminates Kaspersky Endpoint Security setup process.

Using Kaspersky Security Network

At this step, you must either accept or decline the terms of use 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/.

Enter one of the following values:

- `yes` (or `y`), if you accept the terms of the Kaspersky Security Network Statement. Extended KSN mode will be enabled.
- `no` (or `n`), if you do not accept the terms of the Kaspersky Security Network Statement.

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

If Kaspersky Endpoint Security is used in Standard mode and you have enabled the use of Kaspersky Security Network, the application's cloud mode is automatically enabled. In this mode, Kaspersky Endpoint Security uses a lightweight version of the anti-malware databases. Use of the lightweight anti-malware databases is not supported in Light Agent mode for protecting virtual environments.

Removing users from privileged groups

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

At this step, 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.

Assigning the Administrator role to a user

At this step, you can grant the administrator (admin) role to the user.

Enter the name of the user to whom you want to grant the administrator role.

You can grant the administrator role to the user later at any time.

Determining the file operation interceptor type

At this step, the file operation interceptor type for the utilized operating system is determined. For operating systems that do not support fanotify technology, kernel module compilation will begin.

If the necessary packages are not detected during the kernel module compilation process, Kaspersky Endpoint Security will prompt you to install them. If the package download fails, an error message will be displayed.

If all the required packages are available, the kernel module will be automatically compiled when the File Threat Protection task starts.

You can compile the kernel module later after the Kaspersky Endpoint Security initial configuration is complete.

Enabling automatic configuration of SELinux

This step is displayed only if SELinux is installed on your operating system.

At this step, you can enable automatic configuration of SELinux for working with Kaspersky Endpoint Security.

Enter `yes` to enable automatic configuration of SELinux. If SELinux cannot be configured automatically, the application displays an error message and prompts the user to configure SELinux manually.

Enter `no` if you do not want the application to automatically configure SELinux.

By default, the application suggests `yes`.

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

Configuring the update source

This step is displayed only if you selected to use Kaspersky Endpoint Security in Standard mode as a first step. If Kaspersky Endpoint Security is used in Light Agent mode, Kaspersky Endpoint Security receives updates of databases and application modules for the Light Agent from the Protection Server.

At this step, specify the update sources for databases and application modules.

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.
- `< URL >`: the application downloads updates from a custom source. You can specify the address of the custom source of updates in the local area network or on the Internet.
- `< path >` – the application receives updates from the specified directory.

Configuring proxy server settings

This step is displayed only if you selected to use Kaspersky Endpoint Security in Standard mode as a first step.

At this step, you must specify the proxy server settings if you are using a proxy server to access the Internet. Internet connection is required to download the application databases from the update servers.

To configure proxy server settings, perform one of the following actions:

- If you use a proxy server to connect to the Internet, specify the address of the proxy server using one of the following formats:
  - `< IP address of the proxy server >:< port number >`, if the proxy server connection does not require authentication;

- `<user name>:<password>@<IP address of the proxy server>:<port number>`, if the proxy server connection requires authentication.

  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 to connect to the Internet, enter no as your answer.

By default, the application suggests `no`.

You can configure the proxy server settings later without using the initial configuration script.

Starting an application database update

This step is displayed only if you selected to use Kaspersky Endpoint Security in Standard mode as a first step. If Kaspersky Endpoint Security is used in Light Agent mode, Kaspersky Endpoint Security receives updates of databases and application modules for the Light Agent from the Protection Server.

At this step, you can run the application database update task on the client device. 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.

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

If you want to start the database update task on the device, enter `yes`.

By default, the application 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 start the Update task later without using the initial configuration script.

Enabling automatic application database update

This step is displayed only if you selected to use Kaspersky Endpoint Security in Standard mode as a first step. If Kaspersky Endpoint Security is used in Light Agent mode, Kaspersky Endpoint Security receives updates of databases and application modules for the Light Agent from the Protection Server.

At this step, you can enable automatic update of the application databases.

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 without using the initial configuration script by configuring the update task schedule.

Application activation

This step is displayed only if you selected to use Kaspersky Endpoint Security in Standard mode as a first step. If Kaspersky Endpoint Security is used in Light Agent mode, Kaspersky Endpoint Security receives information about the license from the Protection Server; there is no need to activate Kaspersky Endpoint Security separately.

At this step, you can activate the application using an activation code or a key file.

To activate the application using an activation code, enter the activation code.

To activate the application using a key file, specify the full path to the 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 without using the initial configuration script.

Initial configuration of the application in automatic mode

You can perform initial application setup in the automatic mode.

To launch the automatic initial setup of the application, carry out the following command:

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

where < `post-installation configuration file` > is the path to the configuration file that contains the initial configuration settings. You can create this file or copy the necessary structure from the autoinstall.ini configuration file used for remote installation of the application using Kaspersky Security Center.

When the initial setup script is finished and releases the console, the initial setup of the application is complete.

To check the return code, execute the following command:

```
echo $?
```

If the command returns code 0, the initial application setup is finished successfully.

To correctly update application modules after the script has finished, you may need to restart the application. Check the status of updates for the application using the `kesl-control --app-info` command.

Settings in the configuration file for initial setup

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.

Setting	Description	Values
KSVLA_MODE	Kaspersky Endpoint Security usage mode.	yes - Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments (as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent). no - Kaspersky Endpoint Security is used in Standard mode.
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.	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.	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.
EULA_AGREED	Required setting. Acceptance of the terms of the End User License Agreement.	yes: accept the terms of the End User License Agreement to continue the application installation. no – do not accept 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: accept the Privacy Policy to continue installing the application. no: do not accept the Privacy Policy. The application installation will be terminated.
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.	yes – accept the terms of the Kaspersky Security Network Statement and enable the use of KSN. no – do not accept the Kaspersky Security Network Statement.

		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.
GROUP_CLEAN	Required setting. Removing users from the kesladmin and keslaudit privileged groups.	`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` - Do not remove users from the privileged groups.
LOCALE	Optional setting. The locale used for the application events sent to Kaspersky Security Center.	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 fails to determine the operating system localization language or the operating system localization is not supported, the default value will be used – `en_US.utf8`. The locale of the graphical interface and the application command line depends on the value of the `LANG` environment variable. If the locale that is not supported by Kaspersky Endpoint Security is specified as the value of the `LANG` environment variable, the graphical interface and the command line are displayed in English.
INSTALL_LICENSE	Activation code or key file. This setting applies only if the application is used in Standard mode.	
UPDATER_SOURCE	Update source. This setting applies only if the application is used in Standard mode.	`SCServer` – use the Kaspersky Security Center Administration Server as the update source. `KLServers` – use Kaspersky servers as the update source. Update source address
PROXY_SERVER	Address of the proxy server used to connect to the Internet.	Proxy server address

	This setting applies only if the application is used in Standard mode.	
UPDATE_EXECUTE	Start application database update task during setup. This setting applies only if the application is used in Standard mode.	`yes` – start update task. `no` – do not start update task.
KERNEL_SRCS_INSTALL	Automatic start of kernel module compilation.	`yes` – compile kernel module. `no` – do not compile kernel module.
ADMIN_USER	A user assigned the administrator role (admin).	
CONFIGURE_SELINUX	Automatic configuration of SELinux for working with Kaspersky Endpoint Security.	`yes` – automatically configure SELinux to work with Kaspersky Endpoint Security. `no` – do not automatically configure SELinux to work with Kaspersky Endpoint Security.
DISABLE_PROTECTION	Disable protection components and scan tasks after the application is installed. An installation with protection components disabled can be convenient, for example, in order to reproduce a problem in the operation of the application and create a trace file. If you enable the necessary components and tasks after installing the application with the `DISABLE_PROTECTION=yes` parameter, the enabled components and tasks 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.
DISABLE_FILEAV_ACTIONS	Disables the disinfection and file deletion functions for application components after its installation.	`yes`: disables the disinfection and file deletion functions when the application is started after the installation. `no` (default value): does not disable the disinfection and file deletion functions when the application is started after the installation.

	If the disinfection and file deletion functions are disabled and a threat is detected, the application does not attempt to disinfect or delete the files in which a threat was detected, but only informs the user about a threat detection. After installing the application, you can enable the file disinfection and deletion functionality using the `DisableFileAvActions` parameter in the kesl.ini configuration file.	

If you want to change the settings in the configuration file for initial setup of the application, specify the values of settings in the following format: <setting_name>=<setting_value> (the application does not process spaces between the name of a setting and its value).

Configuring permissions in the SELinux system

Manually configuring SELinux for working with the application

If SELinux couldn't s be configured automatically during the initial setup of the application, or if you declined automatic configuration, you can manually configure SELinux to work with Kaspersky Endpoint Security.

To manually configure SELinux to work with the application:

1. Switch SELinux to permissive mode:
   - If SELinux has been activated, run the following command:
     ```
     # setenforce Permissive
     ```
   - If SELinux was disabled, set the `SELINUX=permissive` setting in the configuration file / etc / selinux / config 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 the following Kaspersky Endpoint Security source executable files in accordance with the SELinux policy used:
   - /var/opt/kaspersky/kesl/12.1.0.<build number>_<installation timestamp>/opt/kaspersky/kesl/libexec/kesl
   - /var/opt/kaspersky/kesl/12.1.0.<build number>_<installation timestamp>/opt/kaspersky/kesl/bin/kesl-control
   - /var/opt/kaspersky/kesl/12.1.0.<build number>_<installation timestamp>/opt/kaspersky/kesl/libexec/kesl-gui
   - /var/opt/kaspersky/kesl/12.1.0.<build number>_<installation timestamp>/opt/kaspersky/kesl/shared/kesl

4. Run the following tasks:

   - File Threat Protection task:

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

   - Critical Areas Scan task:

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

   It is recommended to run all the tasks that you plan to run while using Kaspersky Endpoint Security.

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

6. Ensure that there are no errors in 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, and then relaunch all the tasks that you plan to run while using Kaspersky Endpoint Security.

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

8. Switch SELinux to blocking 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 to run the "Start process" task

If SELinux is installed in your operating system in `Enforcing` mode, starting the Start process task requires additional configuration of SELinux.

To configure SELinux to run the "Start process" task

1. Switch SELinux to permissive mode:

   - If SELinux has been activated, run the following command:

     ```
     # setenforce Permissive
     ```

   - If SELinux was disabled, set the `SELINUX=permissive` setting in the configuration file / etc / selinux / config 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. Start the "Start process" task.

4. Ensure that there are no errors in the audit.log file:

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

5. If errors are present in the audit.log file, create and load a new rules module based on blocking rules to fix the errors, then run the "Start process" task again.

6. Switch SELinux to blocking mode:

   ```
   # setenforce Enforcing
   ```

Running the application on Astra Linux OS in closed software environment mode

This section describes how to start the application in the Astra Linux Special Edition operating system.

For Astra Linux Special Edition (operational update 1.7) and Astra Linux Special Edition (operational update 1.6)

To start the application on the Astra Linux Special Edition (operational update 1.7) or Astra Linux Special Edition (operational update 1.6) operating system:

1. Specify the following setting in the /etc/digsig/digsig_initramfs.conf file:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Install the compatibility package:

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

3. Create a directory for the application key:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Locate the application key (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) in the directory created at the previous step:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Update the initramfs image:

   ```
   update-initramfs -u -k all
   ```

For Astra Linux Special Edition (operational update 1.5)

To run the application in the Astra Linux Special Edition (operational update 1.5) operating system:

1. Specify the following setting in the /etc/digsig/digsig_initramfs.conf file:

   ```
   DIGSIG_LOAD_KEYS=1
   DIGSIG_ENFORCE=1
   ```

2. Create a directory for the application key:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

3. Locate the application key (/opt/kaspersky/kesl/shared/kaspersky_astra_pub_key.gpg) in the directory created at the previous step:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

4. Update the initramfs image:

   ```
   sudo update-initramfs -u -k all
   ```

The application graphical user interface can be used during mandatory access control sessions.

Updating the application from a previous version

Only Kaspersky Endpoint Security 12.0 for Linux can be updated to Kaspersky Endpoint Security 12.1 for Linux.

Upgrading earlier Kaspersky Endpoint Security versions to version 12.1 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 12.1 for Linux.

You need to prepare to install before installing Kaspersky Endpoint Security.

The application update procedure involves the following steps:

1. **Updating the Kaspersky Security Center Network Agent**

   If you are managing Kaspersky Endpoint Security using Kaspersky Security Center, you must update the Network Agent on the protected devices. The update is performed by installing a new version of Network Agent.

   If the Network Agent is not updated, the application cannot be managed using Kaspersky Security Center.

   > 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.

   The application continues working correctly during the Network Agent update.

2. **Updating the Kaspersky Endpoint Security administration plug-in**

   If you are managing Kaspersky Endpoint Security using Kaspersky Security Center, you must 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.

3. **Updating the application and graphical user interface on protected devices**

   You must update the application installed on 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 Kaspersky Endpoint Security is being used in Standard mode and you are using the graphical user interface of the application, you must also update the graphical user interface.

   You can update the application and the application's graphical user interface in the following ways:

   - Remotely using Kaspersky Security Center.
   - Locally from the command line.

> 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.

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.

If Kaspersky Endpoint Security is being used in Standard mode, we recommend starting the database update task after updating the application.

Updating Kaspersky Endpoint Security administration 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 administration web plug-in
- Kaspersky Endpoint Security MMC administration plug-in

Policies and tasks configured for Kaspersky Endpoint Security 12.0 for Linux 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 management MMC plug-in, you can convert policies and tasks using the Kaspersky Security Center Policies and Tasks Batch Conversion Wizard (see more details in the Kaspersky Security Center Help).

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.

The procedure for converting policies and tasks is not available in 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.

Administration plug-ins of the previous version continue to work after installing the new version of Kaspersky Endpoint Security administration 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.

Updating the application using Kaspersky Security Center

The application and graphical user interface are updated by remotely installing the new version of the application packages and graphical user interface on the protected device.

The graphical user interface is not supported if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments.

For the remote installation, Kaspersky Endpoint Security installation package is used. You can create the installation package using the Kaspersky Security Center Web Console or the Administration Console.

Kaspersky Security Center Web Console supports the following main deployment methods:

- Installing the application using the Protection Deployment Wizard.

- Installing the application using the remote installation task.

The Kaspersky Security Center Administration Console supports the following main deployment methods:

- Installing the application using the Remote Installation Wizard.
- Installing the application using the remote installation task.

For a description of the deployment procedures, see the Kaspersky Security Center Help.

Updating the application using the command line

Updating the application using the command line is performed by installing a new version of the application on the device from an RPM or DEB format package depending on the type of package manager.

If you are using the graphical user interface, to update it, you must first uninstall the previous version of the graphical user interface package using the command `rpm -e --nodeps kesl-gui`, and then install the package containing files for version 12.1 of the graphical user interface.

> The graphical user interface is not supported if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments.

If the 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 conditions during the update. Read the new version of the End User License Agreement and/or the Privacy Policy:

- The new version of the End User License Agreement is located in the (~/.kesl/<`application version`>/license.<`language ID`>) directory.
- The new version of the Privacy Policy is located in the (~/.kesl/<`application version`>/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. Read the new version of the document located in the (~/.kesl/<`application version`>/ksn_license.<`language ID`>) directory. Refusal to participate in Kaspersky Security Network does not interrupt the Kaspersky Endpoint Security 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.

To accept the conditions of the new agreements during the update, use the environment variables `KESL_EULA_AGREED=yes`, `KESL_PRIVACY_POLICY_AGREED=yes`, and `KESL_USE_KSN=yes/no`.

To update the application:

1. Install the application package using the following command, depending on the package manager. If you have the graphical user interface of the previous version of the application installed, then you also need to start the package containing the files of the graphical user interface.

- for an RPM package.

  ```
  # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] rpm -U --replacefiles --replacepkgs kesl-12.1.0-<build number>.<arch>.rpm [kesl-gui-12.1.0-<build number>.<arch>.rpm]
  ```

  where <arch> is the 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

  On an rpm-based operating system, if the application package and the GUI package are both installed, we do not recommend updating one of the packages without the other.

- for a DEB package:

  ```
  # [KESL_EULA_AGREED=yes] [KESL_PRIVACY_POLICY_AGREED=yes] [KESL_USE_KSN=yes/no] apt-get install ./kesl_12.1.0-<build number>_<arch>.deb [./kesl-gui_12.1.0-<build number>_<arch>.deb]
  ```

  where <arch> is the architecture type:

  - i386 – for 32-bit operating systems
  - amd64 – for 64-bit operating systems
  - arm64 – for 64-bit operating systems for the Arm architecture

  On an dpkg-based operating system, if the application package and the GUI package are both installed, either of the packages cannot be updated without the other.

2. Kaspersky Endpoint Security will restart automatically.
3. Some operating systems may require a restart. The application will show a corresponding message, if necessary.

If you use the command line to manage the application, then after upgrading, most application settings use the values configured for the previous version of the application. Some settings are assigned special values. Settings that were missing in the previous version of the application take on default values in the new version of the application.

Changes to the application settings made after the update is complete and before the application restarts are not saved.

Special considerations when setting parameter values when updating the application

If you use the Kaspersky Security Center Administration Console to manage the application and, after updating the application, you want to use the values of policy and task settings configured in Kaspersky Security Center for the previous version of the application, then you need to convert the policies and tasks (for details, please refer to the Kaspersky Security Center Help).

The procedure for converting policies and tasks is not available in Kaspersky Security Center Web Console. If you use the Web Console to manage your application, you will need to create new policies and tasks for the updated version of the application. You can migrate some settings of policies and tasks from a previous version of a policy or task to a new one by exporting and importing settings.

On the command line, most of the settings are migrated 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.

Exclusion settings

After tasks are converted in the MMC plug-in, the **Use global exclusions** and **Use File Threat Protection exclusions** check boxes are cleared in scan tasks (of the ODS type) and Container Scan tasks. The conversion of tasks is not supported by the web plug-in.

After updating the application on the command line, the `UseOASExclusions` and `UseGlobalExclusions` settings are set to `No`.

Kaspersky Security Network settings

After converting a policy in the MMC plug-in, the **Do not use Kaspersky Endpoint Security** option is selected in the policy properties. The conversion of policies is not supported by the web plug-in.

After upgrading the application on the command line, the `UseKSN` setting is set to `No` if when updating you set `KESL_USE_KSN=No`, and `UseKSN=Extended` is applied if you set `KESL_USE_KSN=Yes`. In other cases, the value of the `UseKSN` setting does not change after the update.

To start or resume using Kaspersky Security Network, you must do the following:

- If using the MMC or web plug-in, select the **Basic KSN mode** or **Extended KSN mode**.
- If using the command line, set `UseKSN` to `Basic` or `Extended`.

Cloud mode settings

After converting a policy in the MMC plug-in, the **Enable cloud mode** check box is cleared. The conversion of policies is not supported by the web plug-in.

After updating the application on the command line, `CloudMode` is set to:

- `CloudMode=No` if `UseKSN=No` after the upgrade.
- `CloudMode=Yes` if `UseKSN=Yes` after the upgrade, and `CloudMode=Yes` was set before the upgrade.

Cloud mode is available if use of KSN is enabled. To enable cloud mode:

- If using the MMC or web plug-in, select the **Extended KSN mode** option and select the **Enable cloud mode** check box.

- If using the command line, set `UseKSN` and `CloudMode` to `Yes`.

File operation interception mode

If the **Block access to files during scans** check box was cleared in the previous version of the application, after converting the policy in the MMC plug-in, the **First action** of the File Threat Protection task is set to **Block**. The conversion of policies is not supported by the web plug-in.

In the new version of the application, the name of the command line option that determines the file operation interception mode has changed from `InterceptorProtectionMode=Block|Notify` to `FileBlockDuringScan=Yes|No`. If in the previous version of the application, `InterceptorProtectionMode` was set to `Notify`, after updating the application using the command line, `FileBlockDuringScan` is set to `No` and the `FirstAction` setting of the File Threat Protection task is set to `Block`.

Uninstalling the application

Uninstalling Kaspersky Endpoint Security involves the following steps:

1. **Uninstalling the application and graphical user interface of the application**

   Uninstall the packages of the application and, if you are using the graphical user interface, the packages of the graphical user interface from the protected devices.

   You can uninstall both the application package and the graphical user interface package, or uninstall only the graphical user interface package. It is not possible to uninstall only the application package if the graphical user interface package is installed.

   You can uninstall the application and the application's graphical user interface in the following ways:

   - Remotely using Kaspersky Security Center.
   - Locally from the command line.

   While the application is being uninstalled, all Kaspersky Endpoint Security tasks will be stopped on the device.

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.

3. **Uninstalling the Kaspersky Endpoint Security administration 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.

After uninstalling the application, all information saved by the application is deleted, except for the license database. Installed application certificates are also removed. The license database is saved, and you can use it to reinstall the application.

If the application was installed in a systemd, the systemd settings are restored to their initial state after the application uninstallation.

Uninstalling the application and Network Agent using Kaspersky Security Center

You can remotely uninstall Kaspersky Endpoint Security and Network Agent from the client devices.

Uninstallation is performed using the remote uninstallation of applications task in Kaspersky Security Center Web Console or in the Administration Console. For more details, refer to the Kaspersky Security Center Help system.

If you want to remove only the graphical user interface without removing the application, specify the `USE_GUI=No` setting value in the autoinstall.ini configuration file and start the remote application installation task.

Uninstallation is performed in the background. After the application uninstallation finishes, you will be prompted to restart the client device.

Uninstalling the application using the command line

Uninstalling the application package and the graphical user interface package

To uninstall the application and the graphical user interface installed from the RPM packages, carry out the following command:

```
# rpm -e kesl kesl-gui
```

To uninstall the application and the graphical user interface installed from the DEB packages, carry out the following command:

```
# apt-get purge kesl kesl-gui
```

Uninstalling the application package without the graphical user interface package

To uninstall the application installed from the RPM package without removing the graphical user interface, carry out the following command:

```
# rpm -e kesl
```

To uninstall the application installed from the DEB package without removing the graphical user interface, carry out the following command:

```
# apt-get purge kesl
```

Removing the graphical user interface package

To remove the graphical user interface that was installed from the RPM package, execute the following command:

```
# rpm -e kesl-gui
```

To remove the graphical user interface that was installed from the DEB package, execute the following command:

```
# apt-get purge kesl-gui
```

After the uninstallation procedure is complete, a message about the results of the uninstallation is displayed.

Network Agent removal using the command line

To uninstall the Network Agent installed on a 32-bit operating system from an RPM package, carry out the following command:

```
# rpm -e klnagent
```

To uninstall the Network Agent installed on a 64-bit operating system from an RPM package, carry out the following command:

```
# rpm -e klnagent64
```

To uninstall the Network Agent installed on a 32-bit operating system from a DEB package, carry out the following command:

```
# apt-get purge klnagent
```

To uninstall the Network Agent installed on a 64-bit operating system from a DEB package, carry out the following command:

```
# apt-get purge klnagent64
```

After the uninstallation procedure is complete, a message about the results of the uninstallation is displayed.

Uninstalling Kaspersky Endpoint Security administration plug-ins

The Kaspersky Endpoint Security web administration plug-in is uninstalled in Kaspersky Security Center Web Console from the list of installed plug-ins (**Settings** → **Web Plug-ins**).

To uninstall the MMC plug-in, use the standard tools for uninstalling applications in the operating system. In the list of applications, select **Kaspersky Endpoint Security <version number> for Linux** to be uninstalled.

Application licensing

This section provides Kaspersky Endpoint Security license information.

About the 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 review the terms of the End User License Agreement for the Kaspersky Endpoint Security solution and the Privacy Policy, which describes the processing and transmission of data, in the following ways:

- By reading the text in the license.<language ID> file. This file is included in the application distribution kit.
- During Kaspersky Endpoint Security installation.

  By confirming your consent to the text of the End User License Agreement and 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 of the End User License Agreement and 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 installing Kaspersky Endpoint Security.

  After the application is installed, the files containing the text of the Kaspersky Endpoint Security End User License Agreement and the Privacy Policy are located on the protected device in the /opt/kaspersky/kesl/doc/license.<language ID> folder.

About the license

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.

The following license types are provided:

- *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 use the application under a trial license for only one trial period.

- *Commercial* is a paid license.

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.

It is recommended to renew the license before its expiration date to ensure continued protection of your device against security threats.

About the license certificate

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

A license certificate contains the following information about the license provided:

- License key or order number
- Information about the license user
- Information about the application that can be activated under the provided license
- Restrictions on the number of licensing units (for example, devices on which the application can be used under the license)
- License validity start date
- License expiration date or validity period
- License type

About the license key

The *license key* is a sequence of bits that can be used to activate the application for further usage in accordance with the terms of the End User License Agreement. License key is generated by Kaspersky experts.

You can add a license key to the application using one of the following methods: by applying a *key file* or by entering an *activation code*. After you add a key to the application, the license key is displayed in the application interface as a unique alphanumeric sequence.

The license key may be blocked by Kaspersky, if the terms of the End User License Agreement are violated. If the license key is blocked, add another license key for proper application operation.

The Kaspersky Endpoint Security application supports the following *types* of license keys:

- *Application key* – a license key for activating the functionality of the Kaspersky Endpoint Security application. The set of available application functions depends on the license associated with the application key.
- *EDR Optimum key* – an additional license key for Kaspersky Endpoint Detection and Response Optimum Add-on in order to activate the functionality of Kaspersky Endpoint Detection and Response Optimum. This key is required if you are using the application under a license that does not include the functionality of Kaspersky Endpoint Detection and Response Optimum.

A license key may be active or reserve.

Active license key is currently used to run the application. A trial license key, commercial license key (commercial key), or subscription key can be added as the active key. Only one active key of each type can be added in the application.

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 license key can be added only if an active license key of the same type is already added.

A trial license key can only be added as an active license key. A trial license key or a subscription key cannot be added as a reserve license key.

About the activation code

An *activation code* is a unique sequence of twenty Latin letters and numbers. You have to enter an activation code in order to add a license key for activating Kaspersky Endpoint Security. You receive the activation code at the email address that you provided when you bought Kaspersky Endpoint Security or requested the trial version of Kaspersky Endpoint Security.

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.

About the key file

A *key file* is a file with the .key extension that you receive from Kaspersky. Key files are intended to add a license key for activating the application.

You receive a key file at the email address that you provided when you bought Kaspersky Endpoint Security or ordered the trial version of Kaspersky Endpoint Security.

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

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.
- Get the key file on the Kaspersky website when you have an activation code.

About subscription

Subscription for Kaspersky Endpoint Security is a purchase order for the application with specific settings (subscription expiry date, number of devices protected). You can order a subscription for Kaspersky Endpoint Security from your service provider (such as your internet service provider). You can renew or cancel your subscription. You can manage your subscription on the website of the service provider.

Subscription can be limited (for one year, for example) or unlimited (without an expiry date). To continue using the application after the limited subscription expires, you need to renew your subscription. Unlimited subscription is renewed automatically if the vendor's services have been prepaid on time.

Upon a limited subscription's expiry, you may be offered a grace period to renew the subscription. During this period the application retains its functionality. The service provider decides whether or not to grant a grace period and, if so, determines the duration of the grace period.

The set of options for managing your subscription may vary depending on your service provider. The service provider might not provide a grace period for renewing the subscription where the application retains its functionality.

To use Kaspersky Endpoint Security under a subscription, you need to use the activation code received from the service provider. After you apply the activation code, an active key corresponding to the license to use the application under subscription is added to the application. A reserve key can only be added when you use an activation code and cannot be added for a key file or subscription.

Activation codes purchased under subscription may not be used to activate previous versions of Kaspersky Endpoint Security.

Comparison of application features across different licenses

The set of application functions available in Kaspersky Endpoint Security depends on the license (see the table below).

Application feature comparison is based on solutions based on Intel architecture processors. For information on licenses and available functionality for solutions based on Arm architecture, please contact your service provider in your region.

Comparison of application functions

Feature	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Endpoint Security for Business Total	Kaspersky Hybrid Cloud Security (Desktop)	Kaspersky Security for Virtualization (Desktop)	Kaspersky Hybrid Cloud Security (Desktop, Enterprise)	Kaspersky Security for Virtualization (Core, Server)
File Threat Protection	✓	✓	✓	✓	✓	✓	✓
Web Threat Protection	✓	✓	✓	✓	✓	✓	✓
Network Threat	✓	✓	✓	✓	✓	✓	✓

Protection							
Firewall Management	✓	✓	✓	✓	✓	✓	✓
Behavior Detection	✓	✓	✓	✓	✓	✓	✓
Device Control	✓	✓	✓	✓	✓	✓	✓
Removable Drives Scan	✓	✓	✓	✓	✓	✓	✓
Anti-Cryptor (for shared folders)	✓	✓	✓	–	–	✓	✓
Container Scan	–	–	–	–	–	✓	–
System Integrity Monitoring	–	–	–	–	–	✓	–
Application Control	–	✓	✓	✓	✓	✓	–
Web Control	✓	✓	✓	✓	✓	✓	✓
Kaspersky Endpoint Detection and Response Optimum Integration	–	–	–	–	–	–	–

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 more 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 KSN Statement, and 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 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 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 used in standard mode and you use Kaspersky update servers to download updates, in order to increase efficiency of the update procedure and to obtain statistical information on the distribution and use 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 to protect virtual environments 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 administration plug-in
    - Web address for downloading the application administration 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
- The current status and execution results of the group and local tasks and the values of their settings
- 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 its application
- 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

If you use Kaspersky Security Network in Extended mode, you agree to automatically submit to Kaspersky all data listed in Kaspersky Security Network Statement. Additionally, files (or parts of files) that intruders may use to harm the device and the data stored in its operating system may be sent to Kaspersky for scanning.

The ksn_license.<language ID> file with the text of the Kaspersky Security Network Statement is included in the application distribution kit.

Data provided when using 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 processed object
  - Attributes of the processed object
  - 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

Application management concept

To manage Kaspersky Endpoint Security, you can use:

- Kaspersky Security Center;
- the command line;
- the graphical user interface.

> If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, it is not possible to manage the application using Kaspersky Security Center Cloud Console and the graphical user interface.

The set of actions that you can perform using the Kaspersky Endpoint Security graphical user interface is limited.

This section describes the specifics of managing the application via Kaspersky Security Center and the command line, and describes the main methods of working in the Kaspersky Security Center administration consoles and in the command line.

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.

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 an MMC administration plug-in for the MMC-based Administration Console (hereinafter also referred to as MMC plug-in).

  > This Help describes how to manage the Administration Console of Kaspersky Security Center 14.2 Windows.

- 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 that has access to the Administration Server.

  The interface for managing Kaspersky Endpoint Security via the Kaspersky Security Center Web Console is provided by a web administration plug-in (hereinafter also simply referred to as web plug-in).

  > This Help describes how to manage the Web Console of Kaspersky Security Center 15.1 Linux.

- 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.

  > The Kaspersky Security Center Cloud Console does not support managing the settings for integrating Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response (KATA).

  > 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 for protecting virtual environments.

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).

Regardless of the Kaspersky Security Center administration console that you use, you must assign the devices on which Kaspersky Endpoint Security is installed to administration groups in order to manage Kaspersky Endpoint Security on these devices using Kaspersky Security Center. 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 Kaspersky Endpoint Security (for details, refer to Kaspersky Security Center documentation).

Kaspersky Endpoint Security administration plug-ins

The following administration plug-ins are required for managing Kaspersky Endpoint Security using Kaspersky Security Center:

- Kaspersky Endpoint Security management web plug-in (hereinafter also referred to as *web plug-in*) facilitates interaction between Kaspersky Endpoint Security and Kaspersky Security Center using Kaspersky Security Center Web Console and Kaspersky Security Center Cloud Console.

  The web plug-in must be installed on the device that has Kaspersky Security Center Web Console installed. Management of Kaspersky Endpoint Security using the web plug-in is available to all administrators who have access to the Kaspersky Security Center Web Console in a browser.

- The Kaspersky Endpoint Security MMC administration plug-in (hereinafter also referred to as the *MMC plug-in*) facilitates interaction between Kaspersky Endpoint Security and Kaspersky Security Center using the Administration Console.

The MMC plug-in must be installed on the device where the Kaspersky Security Center Administration Console is installed.

The Kaspersky Endpoint Security administration plug-ins allow you to manage Kaspersky Endpoint Security using policies and tasks.

For more details about administration plug-ins, refer to Kaspersky Security Center documentation.

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.

Multiple policies with different values of the settings can be configured for a single application. However, there can be only one active policy at a time for an application within an administration group. When you create a new policy, all other policies within an administration group become inactive. You can change the policy status later.

Policies have a hierarchy, similarly to administration groups. By default, a child policy inherits the settings from the parent policy. A *child policy* is a policy of a nested hierarchy level, that is, a policy for nested administration groups and secondary Administration Servers. You can enable inheritance of the settings from the parent policy.

You can locally modify the values of the settings specified by the policy for individual devices within the administration group, if modification of these settings is not prohibited by the policy.

Using policy profiles allows you to flexibly configure operation settings for the application. A *policy profile* may contain 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 operation settings for different devices. You can create and configure profiles in the **Policy profiles** section of the policy properties.

Each policy setting has a "lock" attribute that indicates whether child policy settings and local application settings can be modified. The "lock" status of a setting within policy properties determines whether or not an application setting on a client device can be edited:

- When a setting is "locked" (), you cannot edit its value locally or in the policies of the nested hierarchy level. The setting value specified by the policy is used for all client devices within the administration group and nested groups.
- When a setting is "unlocked" (), you can edit its value locally or in the policies of the nested hierarchy level. If setting values are specified locally or in policy properties of a nested hierarchy level for client devices within an administration group, the setting value specified in the policy properties is not applied.

In the web plug-in and in the MMC plug-in, the number of parameters with "locks" is different. The web plug-in includes "locks" that are not present in the MMC plug-in.

After the policy is applied for the first time, the application settings change in accordance with the policy settings.

For more details about policies and policy profiles, refer to the Kaspersky Security Center Help system.

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 sets of devices to run on multiple devices, regardless of their inclusion in administration groups.

  The tasks for the sets of devices are performed only on the devices that are specified in the task settings. If new devices are added to the device selection for which the task is created, this task is not applied to the new devices. To apply the task to these computers, you must create a new task or edit the settings of the existing task.

You can create any number of group tasks, tasks for a sets of devices, or local tasks.

The tasks are executed only if Kaspersky Endpoint Security is running on the devices.

General information about tasks created in Kaspersky Security Center is provided in Kaspersky Security Center documentation.

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.
- **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.

The set of policy settings and default values for task settings depend on the license type. The Add Key, Update and Rollback tasks are not applicable if the application is used in Light Agent mode to protect virtual environments. Additionally, some application functions are not supported in a KESL container.

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.

To log in to Web Console:

1. In your browser, go to the `<Administration Server web address>:<port number>` address.

   The login page is displayed.

2. 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.

3. Click **Log in**.

   If the Administration Server is not responding, or if you enter incorrect credentials, an error message is displayed.

After logging in, a dashboard is displayed with the last language and theme used.

For more details about the Web Console interface, refer to Kaspersky Security Center documentation.

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 the Kaspersky Security Center Cloud Console documentation.

Managing policies in the Web Console

You can perform the following actions with the policies in the Web Console:

- Create a policy.
- Edit policy settings.

> If the user account which is used to access the Administration Server does not have permissions to edit the settings of certain functional scopes, the settings of these functional scopes are not available for editing. Configuration of some settings is not supported in the KESL container.

- Export and import policy settings.
- Copy and move a policy.
- Delete a policy.
- Change a policy status.
- Create policy profiles.

For general information about working with policies, refer to the Kaspersky Security Center Help system.

Creating a policy in the Web Console

To create a policy in the Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Policies and policy profiles**.

   A list of policies and policy profiles opens.

2. Select the administration group containing the devices to which the policy should be applied. To do so, click the link in the **Current path** field located above the list of policies and policy profiles, and select the administration group in the window that opens.

3. Click **Add**.

   The Policy Wizard starts.

4. In the drop-down list, select **Kaspersky Endpoint Security 12.1 for Linux**.

   Proceed to the next step of the wizard.

5. Specify the Kaspersky Endpoint Security usage mode:

   - **Standard mode to protect workstations and servers** – the application is used to protect devices running Linux operating systems.
   - **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.

6. If you are using the application in Light Agent mode to protect virtual environments, configure the SVM discovery settings:

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

   - **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.

   - **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 advanced 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 SVM path**. If any other value is set, Light Agents will not be able to connect to the SVM.

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 a NetBIOS name, "localhost", or 127.0.0.1 is specified as the address, the connection to the Integration Server fails with an error.

- **Port**

  Port for connecting to the Integration Server.

  Port 7271 is used by default.

b. Click the **Check** button.

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 **Connection to the Integration Server** 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, the window displays 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 multiple IP addresses or FQDNs of SVMs on 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 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. 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**. The policy that is not currently applied to the device. If this option is selected, the policy becomes inactive but remains in the **Policies** folder. You can activate the inactive policy later.
   - Policy settings inheritance:
     - **Inherit settings from parent policy**. If this option is enabled, the policy settings values are inherited from the upper-level group policy and, therefore, are locked. This toggle switch is turned on by default.
     - **Enforce settings inheritance for child policies** If this option is enabled, the settings values of the child policies are locked. This toggle switch is turned off by default.

   For general information about the policy settings, refer to Kaspersky Security Center Help section.

9. If you want to configure other policy settings, go to the **Application settings** tab and make the necessary changes.

   You can also change the policy settings later.

10. Click **Save**.

The created policy will be displayed in the list of policies.

For general information about managing policies, refer to the Kaspersky Security Center Help system.

Changing policy settings in the Web Console

To edit policy settings in the Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Policies and policy profiles**.

   The list of policies opens.

2. Select the administration group containing the devices to which the policy is applied. To do so, click the link in the **Current path** field in the upper part of the window and select the administration group in the window that opens.

   The list displays the policies configured for the selected administration group.

3. Click the name of the required policy in the list.

   The policy properties window opens.

4. Modify the policy settings on the **Application settings** tab.

5. Click the **Save** button to save the changes made.

The policy is saved with the updated settings.

Policy settings in the Web Console

The default set of settings and values for the policy settings depend on the license that was used to activate the application. Some policy settings are applied or not applied to the application depending on the application mode. Additionally, some application functions are not supported in a KESL container.

You can configure policy settings on the **Application settings** tab of the policy properties window.

Policy settings

Section	Subsections
Essential Threat Protection	File Threat Protection File Threat Protection exclusions Firewall Management Web Threat Protection Network Threat Protection
Advanced Threat Protection	Kaspersky Security Network Anti-Cryptor Behavior Detection
Detection and Response	Managed Detection and Response Endpoint Detection and Response Optimum Endpoint Detection and Response (KATA)
Security Controls	Application Control

	Device Control System Integrity Monitoring Web Control
Local Tasks	Task management Removable Drives Scan
General settings	Proxy server settings Application settings Container Scan settings Network settings Global exclusions Storage settings
Light Agent mode	SVM discovery settings Integration Server connection settings SVM connection tag SVM selection algorithm Protecting the connection

Managing policies in the Administration Console

You can perform the following actions with the policies in the Kaspersky Security Center Administration Console:

- Create a policy.
- Edit policy settings.

  If the user account which is used to access the Administration Server does not have permissions to edit the settings of certain functional scopes, the settings of these functional scopes are not available for editing. Configuration of some settings is not supported in the KESL container.

- Export and import policy settings.
- Delete a policy.
- Change a policy status.
- Create policy profiles.

For general information about working with policies, refer to the Kaspersky Security Center Help system.

Creating a policy using the Administration Console

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. In the first step of the Wizard, select **Kaspersky Endpoint Security 12.1 for Linux** from the list.

   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:

   - **Standard mode to protect workstations and servers** – the application is used to protect devices running Linux operating systems.

   - **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 to protect virtual environments, configure the SVM discovery settings:

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

   - **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.

- **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 advanced 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 SVM path**. If any other value is set, Light Agents will not be able to connect to the SVM.

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 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 a NetBIOS name, "localhost", or 127.0.0.1 is specified as the address, the connection to the Integration Server fails with an error.

   - **Port**

     Port for connecting to the Integration Server.

     Port 7271 is used by default.

   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, the window displays 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 multiple IP addresses or FQDNs of SVMs on 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. 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.

You can change the policy settings later. For general information about managing policies, refer to the Kaspersky Security Center Help system.

Changing policy settings in the Kaspersky Security Center Administration Console

To edit policy 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. Edit the policy settings.

5. In the **Properties: <Policy name>** window, click **OK** to save the changes.

Policy settings in the Administration Console

The default set of settings and values for the policy settings depend on the license that was used to activate the application. Some policy settings are applied or not applied to the application depending on the application mode. Additionally, some application functions are not supported in a KESL container.

You can configure policy settings in the sections and subsections of the policy properties window. For information about configuring general policy settings and event settings, refer to Kaspersky Security Center Help section.

Policy settings

Section	Subsections
Essential Threat Protection	File Threat Protection File Threat Protection exclusions Firewall Management Web Threat Protection Network Threat Protection
Advanced Threat Protection	Kaspersky Security Network Anti-Cryptor Behavior Detection
Detection and Response	Managed Detection and Response Endpoint Detection and Response (KATA)
Security Controls	Application Control Device Control System Integrity Monitoring Web Control
Local Tasks	Task management Removable Drives Scan
General settings	Proxy server settings Application settings Container Scan settings Network settings Global exclusions Excluding process memory

	Storage settings
Light Agent mode	Connection to the Integration Server SVM discovery settings SVM connection tag SVM selection algorithm Protecting the connection

Managing tasks in the Web Console

You can perform the following actions with the tasks for Kaspersky Endpoint Security in the Web Console:

- Create new tasks.
- Edit task settings.

  If the user account which is used to access the Administration Server does not have permissions to edit the settings of certain functional scopes, the settings of these functional scopes are not available for editing. Configuration of some settings is not supported in the KESL container.

- Start, stop, pause, and resume tasks.

  The *Update* task cannot be paused or resumed, it can only be started or stopped.

- Export and import tasks.
- Delete tasks.

In the list of tasks, you can monitor the task execution results, which include the task status and the statistics for task performance on the devices. You can also create a selection of events to monitor the task execution (**Monitoring and reports** → **Event selections**). For details on event selection, refer to Kaspersky Security Center documentation.

Task execution results are also saved locally on the device and in Kaspersky Security Center reports.

For general information about task management, refer to the Kaspersky Security Center Help system.

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 local user interface on the device.

Creating tasks in the Web Console

To create a task in the Web Console:

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

The list of tasks opens.

2. Click **Add**.

   The Task Wizard starts.

3. In the first step of the Wizard, perform the following actions:

   a. In the **Application** drop-down list, select **Kaspersky Endpoint Security 12.1 for Linux**.

   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 configure the task settings immediately after creation, in the last step of the Wizard, select the **Open task properties window after creation** check box. A task is created with the default settings.

6. Complete the wizard.

A new task will be displayed in the list of tasks.

Changing task settings in the Web Console

To edit task settings in the Web Console:

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

   The list of tasks opens.

2. Do one of the following:

   - To edit the settings of a task that is run on all devices included in a specific administration group, click the link in the **Current path** field in the upper part of the window and select the administration group in the window that opens.

     The list displays only tasks configured for the selected administration group.

   - To edit the settings of a task that is run on one or multiple devices (a task for a set of devices), click the link in the **Current path** field in the upper part of the window and select the top node with the name of the Administration Server in the window that opens.

     The list displays all tasks created on the Administration Server.

3. In the list of tasks, select the required task and open the task properties window by clicking the link in the task name.

4. Configure the task settings:

   - On the **General** tab, you can edit the name of the task.

   - On the **Application settings** tab, you can configure specific task settings. The availability of configurable settings depends on the type of task.

   - On the **Schedule** tab, you can configure the task run schedule and additional settings for starting and stopping the task.

   The **General**, **Results**, **Settings**, **Schedule**, and **Revision history** tabs of the task properties window are standard for Kaspersky Security Center; for more details, refer to the Kaspersky Security Center Help system.

5. Click the **Save** button to save the changes made.

Starting, stopping, pausing, and resuming tasks in the Web Console

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 specific administration group, click the link in the **Current path** field in the upper part of the window and select the administration group in the window that opens.

     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 link in the **Current path** field in the upper part of the window and select the top node with the name of the Administration Server in the window that opens.

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.

Managing tasks in the Administration Console

You can perform the following actions with the tasks for Kaspersky Endpoint Security in the Administration Console:

- Create new tasks.
- Edit task settings.

  If the user account which is used to access the Administration Server does not have permissions to edit the settings of certain functional scopes, the settings of these functional scopes are not available for editing. Configuration of some settings is not supported in the KESL container.

- Start, stop, pause, and resume tasks.

  The *Update* task cannot be paused or resumed, it can only be started or stopped.

- Export and import tasks.
- Delete tasks.

In the list of tasks, you can monitor the task execution results, which include the task status and the statistics for task performance on the devices.

Information on the progress and results of task execution can be viewed in the list of events that Kaspersky Endpoint Security sends to the Kaspersky Security Center Administration Server (on the **Events** tab in the workspace of the **Administration Server <server name>** node). You can also create a selection of events to monitor the execution of tasks. For details on event selection, refer to Kaspersky Security Center documentation.

Task execution results are also saved locally on the device and in Kaspersky Security Center reports.

For general information about task management, refer to the Kaspersky Security Center Help system.

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 local user interface on the device.

Creating tasks in the Administration Console

To create a task 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. In the first step of the Wizard, select **Kaspersky Endpoint Security 12.1 for Linux** and the type of the task.

   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 system).

   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. Complete the wizard.

   A new task will be displayed in the list of tasks.

Changing task settings in the Administration Console

To edit task settings 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 the required task and double-click it to open the **Properties: <Task name>** window.

   You can also open the task properties window using the **Properties** item in the task context menu.

3. Edit the task settings. The availability of configurable settings depends on the type of task.

   The **General**, **Notification**, **Schedule**, and **Revision history** tabs of the task properties window are standard for Kaspersky Security Center; for more details, refer to the Kaspersky Security Center Help system.

4. Click **Apply** or **OK** in the **Properties: <Task name>** window to save the changes made.

Starting, stopping, pausing, and resuming tasks in the Administration Console

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.

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.

The functional components of the application are supported by *Kaspersky Endpoint Security local tasks* that are run in the operating system. You can enable or disable functional components of the application on a device by starting or stopping Kaspersky Endpoint Security tasks in the command line. One-time device scans are also performed by starting Kaspersky Endpoint Security tasks. You can define the settings for functional components on the device and the device scan settings by configuring the Kaspersky Endpoint Security *task settings*.

In addition to the task settings, the following settings are provided for configuring the application:

- General Container Scan settings.
- Encrypted connections scan settings.

- General application settings that define the operation of the application as a whole and the operation of individual functions.

In the command line, Kaspersky Endpoint Security is managed using *Kaspersky Endpoint Security management commands*.

Enabling automatic addition of kesl-control commands (bash completion)

Automatic addition of kesl-control commands can be disabled for the bash shell.

To enable automatic addition of kesl-control commands in the current bash shell session, run the following command:

```
source /opt/kaspersky/kesl/shared/bash_completion.sh
```

To enable automatic addition for all new bash shell sessions, run the following command:

```
echo "source /opt/kaspersky/kesl/shared/bash_completion.sh" >> ~.bashrc
```

Task management in the command line

The following application tasks are provided for managing Kaspersky Endpoint Security using the command line:

- *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. The task starts automatically when the application starts.
- *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.
- *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.
- *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.
- *Container scan*. This task allows you to scan containers and images on demand and defines the settings for the scan.
- *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.
- *Removable Drives Scan*. This task allows you to monitor the connection of removable drives to the device in real time and defines the settings for the removable drives scan, as well as the scan of their boot sectors, for the presence of malware.
- *Web Threat Protection*. This task allows you to enable or disable Web Threat Protection and defines the settings for the Web Threat Protection component.

- *Network Threat Protection*. This task allows you to enable or disable Network Threat Protection and defines the settings for the Network Threat Protection component.
- *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.
- *Firewall Management*. This task allows you to enable or disable firewall management and defines the network connection control settings on the device.
- *Application Control*. This task allows you to enable or disable Application Control and defines the settings of the Application Control component.
- *Inventory*. The task allows you to obtain information about all the application executable files stored on the device.
- *Device Control*. This task allows you to enable or disable Device Control and defines the settings for the Device Control component. The task starts automatically when Kaspersky Endpoint Security starts.
- *Web Control*. This task allows you to enable or disable Web Control and defines the settings of the Web Control component.
- *Behavior Detection*. This task allows you to monitor malicious activity of applications in the operating system. The task starts automatically when Kaspersky Endpoint Security starts.
- *System Integrity Monitoring*. This task allows you to perform real-time monitoring of the actions performed with objects from the monitoring scope specified in the System Integrity Monitoring component settings.
- *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.
- *Backup management*. This task provides the capability to save backup copies of files to the Backup located on the device. The task starts automatically when the application starts, and it resides in the device operating memory. The task cannot be started, stopped, or deleted.
- *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.
- *Update*. You can use this task to perform scheduled and on-demand application database and module updates and edit update settings.
- *Rollback*. You can use this task to roll back the last update of application databases and modules.
- *Kaspersky Endpoint Detection and Response (KATA) Integration*. This task allows you to enable or disable integration with Kaspersky Endpoint Detection and Response (KATA) and defines the integration settings.

Each application task has a name used on the command line, an ID, and a type (see the table below).

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 name in command line	Task ID	Task type
File Threat Protection	File_Threat_Protection	1	OAS
Malware Scan	Scan_My_Computer	2	ODS
Malware Scan (user task)	user-defined	starting from 100	ODS
Custom file scan	Scan_File	3	ODS
Critical Areas Scan	Critical_Areas_Scan	4	ODS
Container Scan	Container_Scan	18	ContainerScan
Container scan (user task)	user-defined	starting from 100	ContainerScan
Custom Container Scan	Custom_Container_Scan	19	ContainerScan
Removable Drives Scan	Removable_Drives_Scan	16	RDS
Web Threat Protection	Web_Threat_Protection	14	WTP
Network Threat Protection	Network_Threat_Protection	17	NTP
Anti-Cryptor	Anti_Cryptor	13	AntiCryptor
Firewall Management	Firewall_Management	12	Firewall
Application Control	Application_Control	21	AppControl
Inventory	Inventory_Scan	22	InventoryScan
Inventory (user task)	user-defined	starting from 100	InventoryScan
Device Control	Device_Control	15	DeviceControl
Behavior Detection	Behavior_Detection	20	BehaviorDetection
System Integrity Monitoring	System_Integrity_Monitoring	11	OAFIM
System Integrity Monitoring (user task)	user-defined	starting from 100	ODFIM
Backup management	Backup	10	Backup
Update	Update	6	Update
Update (user task)	user-defined	starting from 100	Update
Rollback	Rollback	7	Rollback
Rollback (user task)	user-defined	starting from 100	Rollback
Licensing	License	9	License
Kaspersky Endpoint Detection and	KATAEDR	24	KATAEDR

Response (KATA) Integration			
Web Control	Web_Control	26	WebControl

You can perform the following actions with tasks:

- Start and stop all predefined and user tasks except *Backup* and *License* tasks.
- Suspend and resume *ODS*, *ODFIM*, and *InventoryScan* tasks.
- Create and delete user tasks. Depending on the application usage mode, you can create the following types of tasks:
  - Standard mode: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan*, and *InventoryScan*;
  - Light Agent mode for protecting virtual environments: *ODS*, *ODFIM*, *ContainerScan*, and *InventoryScan*.
- Change the settings for all user tasks and all predefined tasks, except for *Rollback* and *License* tasks.

  If the application is used in Light Agent mode to protect virtual environments, the settings of the predefined *Update* task also cannot be edited.

- Configure the task start schedule.

Viewing a list of tasks in the command line

To view the list of application tasks, execute the following command:

```
kesl-control --get-task-list [--json]
```

where:

`--json` – output format for the list of application tasks. If a file format is not specified, the output will be an INI file.

The list of Kaspersky Endpoint Security tasks will be displayed.

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 Kaspersky Security Center policy prohibits users from viewing and editing tasks locally, information will only be displayed about the *Scan_File*, *Backup*, *License*, *File_Threat_Protection*, *System_Integrity_Monitoring*, and *Anti_Cryptor*. tasks. Information about other tasks is not available.

Viewing the status of a task in the command line

To view a task state, execute the following command:

```
kesl-control --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 in the command line.
- `--json` is specified to output the settings in JSON format.

Application tasks can take the following main states:

- `Started`—Task is running.
- `Starting`—Task is being launched.
- `Stopped`—Task has been stopped.
- `Stopping`—Task is stopping.

The *ODS*, *ODFIM*, and *InventoryScan* tasks can also have one of the following states:

- `Pausing` — Task is pausing.
- `Suspended` — Task is suspended.
- `Resuming` — Task is resuming.

Creating a task in the command line

If the application is being used in standard mode, you can create the following types of tasks: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan*, and *InventoryScan*.

If the application is used in Light Agent mode to protect virtual environments, you can create the following types of tasks: *ODS*, *ODFIM*, *ContainerScan*, and *InventoryScan*.

You can create tasks with default settings or with settings specified in a configuration file.

To create a task with default settings, execute the following command:

```
kesl-control -create-task <task name> --type <task type>
```

where:

- `< task name >` is the name that you specify for the new task.
- `< task type >` is the identifier for the type of the created task.

To create a task with the settings specified in the configuration file, execute the following command:

```
kesl-control --create-task < task name > --type < task type > --file < path to the
configuration file > [--json]
```

where:

- `< task name >` is the name that you specify for the new task.
- `< task type >` is the identifier for the type of the created task.
- `< 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` key is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

Starting, stopping, pausing, and resuming tasks in the command line

You can start and stop predefined and user tasks, except for tasks of *Backup* and *License* types.

You can suspend and resume tasks of *ODS*, *ODFIM*, and *InventoryScan* types.

To start a task, execute 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 in the command line.
- `[-W]` is a command used in conjunction with the task start command to enable the display of current events associated with this task.
- `[--progress]` is a key that must be specified if you want to display the progress of the task.

  Example:
  Start the task with ID 1 and enable the display of current events associated with the task:

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

To stop a task, execute the following command:

```
kesl-control --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 in the command line.
- `[-W]` is a command used in conjunction with the stop task command to enable the display of current events associated with this task.

To suspend a task, execute the following command:

```
kesl-control --suspend-task < task ID/name >
```

To resume a task, execute the following command:

```
kesl-control --resume-task < task ID/name >
```

Deleting a task in the command line

You can delete only user tasks. Predefined tasks cannot be deleted.

To delete a task, execute the following command:

```
kesl-control --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 in the command line.

Displaying task settings in the command line

You can display the current values of settings for all user tasks and all predefined tasks, except for *Rollback* and *License* tasks (these tasks have no settings).

You can output the current values of task settings to the console or to a configuration file that you can use to change task settings.

To output the current values of task settings to the console, execute the following command:

```
kesl-control --get-settings < 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 in the command line.
- `--json` is specified to output the settings in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

To output the current values of task settings to a configuration file, execute the following command:

```
kesl-control --get-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 in the command line.
- `--file <configuration file path>` – path to the configuration file into which the task settings will be written. 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` key is not specified, the settings will be imported in the INI format.

Editing task settings in the command line

You can edit the settings for all user tasks and all predefined tasks, except for *Rollback* and *License* tasks.

> If the application is used in Light Agent mode to protect virtual environments, the settings of the predefined *Update* task also cannot be edited.

In the command line, you can edit the settings of tasks using the `kesl-control --set-settings` command:

- You can edit all task settings using the configuration file that contains the task settings. You can get the configuration file using the command for displaying task settings.
- You can edit individual task settings using command line keys in the format `<setting name>=<setting value>`. You can get the current values of task settings using the command for displaying task settings.
- You can restore the task settings to their default values.

You can add or remove scan scopes and exclusion scopes using a configuration file that contains task settings or command line keys. Configuring scan scopes and exclusion scopes is available for tasks with the *OAS*, *ODS*, *OAFIM*, *ODFIM*, and *AntiCryptor* types.

> 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/`.

For some tasks, separate management commands are also provided that allow you to edit task settings.

Editing task settings using a configuration file

To edit values of task settings using a configuration file:

1. Output the task settings to the configuration file using the command `kesl-control --get-settings`.

2. Open the configuration file and edit the values of the necessary settings.

   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. Save the configuration file.

4. Execute the 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 in the command line.
   - `--file <configuration file path>` – full path to the configuration file from which the task settings will be imported.

- `--json`: specify this key if you are importing settings from a configuration file in JSON format. If the `--json` key 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` key.

Editing task settings using the command line keys

Using the `kesl-control --set-settings` command keys, you can edit individual values of task settings, as well as add or remove scan scopes and exclusion scopes for tasks of the *OAS*, *ODS*, *OAFIM*, *ODFIM*, and *AntiCryptor* types.

Configuring individual task settings

To edit individual values of task settings using command line keys, execute the following 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 in the command line.
- `<setting name>=<setting value>` is the name and value of one of the task settings. 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` key.

Adding and removing a scan scope

To add a scan scope using command line keys, execute the following command:

```
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 in the command line.
- --add-path < path > adds the path to the directory with the objects to be scanned.

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. The remaining settings of the scan scope take default values.

If the task settings already contain a [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:
Adding a scan scope for a task with ID=100:

```
kesl-control --set-settings 100 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=

UseScanArea=Yes

Path=/home

AreaMask.item_0000=*
```

To delete a scan scope using command line keys, execute the following command:

```
kesl-control --set-settings < task ID/name > --del-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 in the command line.
- --del-path < path > deletes the path to the directory with the objects to be scanned.

The [ScanScope.item_#] section that contains the specified path will be deleted from the task settings. The application will not scan the objects in the specified directory.

Adding and removing an exclusion scope

To add an exclusion scope using command line keys, execute 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 in 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.

To delete an exclusion scope using command line keys, execute 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 in the command line.
- `--del-exclusion < path >` deletes the path to the directory with the objects to be excluded.

  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.

Restoring default task settings in the command line

You can restore the default settings for all user tasks and all predefined tasks, except for tasks of the *Rollback* and *License* types (these tasks have no settings).

To reset task settings to their default values, execute the following 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 in the command line.

The application changes the setting values to their defaults.

Configuring task schedule in the command line

If the application is being used in standard mode, you can configure the run schedule for the following types of tasks: *ODS*, *Update*, *Rollback*, *ODFIM*, *ContainerScan*, and *InventoryScan*.

If the application is used in Light Agent mode to protect virtual environments, you can configure the run schedule for the following types of tasks: *ODS*, *ODFIM*, *ContainerScan*, and *InventoryScan*.

You can output the current values of the settings for the task run schedule to the console or to a configuration file.

To output the current settings for the task run schedule to the console, execute the following command:

```
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 in the command line.
- `--json` is specified to output the settings in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

To output the current settings for the task run schedule to a configuration file, execute the following command:

```
kesl-control --get-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 in the command line.
- `--file <path to configuration file>` is the path to the configuration file in which the settings for the task run schedule will be output. 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` key is not specified, the settings will be imported in the INI format.

  Examples:
  Save the update task settings to a file named update_schedule.ini and save the created file in the current directory:

  ```
  kesl-control --get-schedule 6 --file update_schedule.ini
  ```

  Display the update task schedule in the console:

  ```
  kesl-control --get-schedule 6
  ```

You can edit the settings for the task run schedule in the following ways:

- Import the settings from a configuration file that contains all schedule settings.
- Using the command line, specify the individual settings for the task run schedule in the format `<setting name>=<setting value>`.

To edit the values of the settings for task run schedule using a configuration file, perform the following actions:

1. Output the task settings to the configuration file using the command `kesl-control --get-schedule`.
2. Edit the values of the necessary settings in the file and save the changes.
3. Execute the command:

   `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 in the command line.

   `--file <configuration file path>` – full path to the configuration file from which the task schedule settings will be imported.

   `--json`: specify this key if you are importing settings from a configuration file in JSON format. If the `--json` key is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

   All values of the settings for the task run schedule defined in the file will be imported into the application.

Example:
Import the schedule settings from the configuration file named /home/test/on_demand_schedule.ini into the task with ID=2:

```
kesl-control --set-schedule 2 --file /home/test/on_demand_schedule.ini
```

To edit the individual values of the settings for the task run schedule using the command line, execute the following command:

```
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 in the command line.
- `<setting name>=<setting value>` is the name and value of one of the settings for the task schedule.

The values of the specified settings for the task run schedule are modified.

Examples:
To schedule the task to start every ten hours, specify the following settings:

```
RuleType=Hourly

RunMissedStartRules=No

StartTime=2021/May/30 23:05:00;10

RandomInterval=0
```

To schedule the task to start every ten minutes, specify the following settings:

```
RuleType=Minutely

RunMissedStartRules=No

StartTime=23:10:00;10

RandomInterval=0
```

To schedule the task to start on the 15th of every month, specify the following settings:

```
RuleType=Monthly

RunMissedStartRules=No

StartTime=23:25:00;15

RandomInterval=0
```

To schedule the task to start on every Tuesday, specify the following settings:

```
RuleType=Weekly

StartTime=18:01:30;Tue

RandomInterval=99

RunMissedStartRules=No
```

To schedule the task to start every 11 days, specify the following settings:

```
RuleType=Daily

RunMissedStartRules=No

StartTime=23:15:00;11

RandomInterval=0
```

Managing general application settings in the command line

General application settings define the operation of the application as a whole and the operation of individual functions.

You can manage general application settings using special management commands:

- Output the current values of general application settings to the console or to a configuration file.
- Edit general application settings using a configuration file containing all general settings, or using command line keys in the format <setting name>=<setting value>.

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 Scan 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.

Displaying general application settings

You can output the current values of general application settings to the console or to a configuration file that you can use to edit task settings.

To output the current values of general application settings to the console, execute the following command:

```
kesl-control --get-app-settings [--json]
```

where `--json` is specified to output the settings in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

To output the current values of general application settings to a configuration file, execute the following command:

```
kesl-control --get-app-settings --file <configuration file path> [--json]
```

where:

- `--file <configuration file path>` – path to the configuration file into which general settings of the application will be written. 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` key is not specified, the settings will be imported in the INI format.

  Example:
  Display the general application settings to a file named kesl_config.ini. Save the created file in the current directory:
  `kesl-control --get-app-settings --file kesl_config.ini`

Editing general application settings

In the command line, you can edit the general application settings using the command `kesl-control --set-app-settings`:

- You can edit all general settings using the configuration file that contains the general application settings. You can get the configuration file using the command for displaying general settings.
- You can edit individual settings using command line keys in the format < `setting name` >=< `setting value` >. You can get the current values of general application settings using the command for displaying general settings.

To edit values of general application settings using a configuration file:

1. Output the general application settings to a configuration file.
2. Edit the values of the necessary parameters in the file and save the changes.
3. Execute the command:

   `kesl-control --set-app-settings --file < configuration file path > [--json]`

   where:

   - `--file < path to configuration file >` is the full path to the configuration file with the general application settings.
   - `--json`: specify this key if you are importing settings from a configuration file in JSON format. If the `--json` key 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.

To edit values of general application settings using command line keys, execute the following command:

`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 general application settings.

The values of the specified general settings will be changed.

Examples:

Import general settings into the application from the configuration file /home/test/kesl_config.ini:

```
kesl-control --set-app-settings --file /home/test/kesl_config.ini
```

Set the detail level for the trace file to low:

```
kesl-control --set-app-settings TraceLevel=NotDetailed
```

Add a mount point that you want to exclude from interception of file operations:

```
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:

```
"<field> <comparison operator> '<value>'"
```

```
"<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 operators:
  - `>` 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"
  - `==` 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 in 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.

You can use a filter in the following application management commands:

- Display information about certain current events of the application:

  ```
  kesl-control -W --query "<filter conditions>"
  ```

- Display information about certain application events in the event log:

  `kesl-control -E --query "< filter conditions >"`

- Display information about certain objects in the Backup:

  `kesl-control -B --query "< filter conditions >"`

- Delete certain objects from the Backup:

  `kesl-control -B --mass-remove --query "< filter conditions >"`

  Examples:
  Get information about events that contain the text "etc" in the FileName field:
  `kesl-control -E --query "FileName like '%etc%'"`
  Display information about events with the ThreatDetected type:
  `kesl-control -E--query "EventType == 'ThreatDetected'"`
  Display information about events with the ThreatDetected type, created by tasks of the ODS type:
  `kesl-control -E --query "EventType == 'ThreatDetected' and TaskType == 'ODS'"`
  Get 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'"`
  Get 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'"`
  Get information about files in the Backup storage that have the High severity level:
  `kesl-control -B --query "DangerLevel == 'High'"`

Exporting and importing application settings

If Kaspersky Endpoint Security is managed via Kaspersky Security Center, importing settings is not supported.

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the settings of the predefined task of the *Update* type cannot be exported or imported.

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. When exporting settings, all application settings (including general Container Scan settings, encrypted connections scan settings, general application settings, and task settings) are saved in a configuration file. You can use this configuration file to import settings into the application.

The application must be launched when settings are imported or exported. After the settings are imported, the application must be restarted.

When importing or exporting settings from an older application version, new settings are set to default values. Importing settings to an older application version is not supported.

To export the application settings, execute the following command:

`kesl-control --export-settings --file < configuration file path > [--json]`

where:

- `--file <configuration file path>` – full path to the configuration file where the application settings will be saved.
- `--json` is specified to export the settings to the configuration file in JSON format. If the `--json` key is not specified, the settings will be exported to an INI file.

To import the application settings from the file, execute the following command:

```
kesl-control --import-settings --file <configuration file path> [--json]
```

where:

- `--file <configuration file path>` – full path to the configuration file to import the settings into the application.
- `--json` is specified to import the settings from the configuration file in JSON format. If the `--json` key is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

When you import application settings from a file, the `UseKSN` and `CloudMode` settings are set to `No`. To start or resume the use of Kaspersky Security Network, set the value of the `UseKSN` setting to `Basic` or `Extended`. To enable cloud mode, you must set the `CloudMode` setting to `Yes`. Cloud mode is available if use of KSN is enabled.

After application settings are imported, internal task IDs may change. It is recommended to use task names to manage tasks.

Managing user roles using the command line

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*, and *nokesl*. When you assign an application role to a system user, the user is added to the corresponding group of roles (see the *Roles* table below). When you revoke a role from a user, this user is removed from the corresponding group of roles.

If no application role is assigned to a system user, that user belongs to a separate group of *users without rights*.

Thus, the roles correspond to the four groups of operating system users:

- kesladmin – the Administrator role
- kesluser – the User role
- keslaudit – the Auditor role
- nokesl is assigned to a user if no other roles are assigned. In this case, the user belongs to a separate group of *users without privileges*

User roles

Role name	Role in application	OS user	Permissions
Administrator	admin	kesladmin	Manage application settings and task settings. Manage application licensing. Assigning roles to users. Revoking user roles (the administrator has no right to revoke the admin role from himself). View and manage users' Storages.
User	user	kesluser	Manage only user file scan tasks. Start and stop Update tasks. 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.

Viewing a list of users and roles

To view a list of users and their roles, execute the following command:

```
kesl-control [-U] --get-user-list
```

Assigning a role to a user

To assign a role to a specific user, execute the following command:

```
kesl-control [-U] --grant-role <role> <user>
```

Example:
To assign the audit role to the user test15:

```
kesl-control --grant-role audit test15
```

Revoking a user role

To revoke a role from a specific user, execute the following command:

```
kesl-control [-U] --revoke-role <role> <user>
```

Example:

To revoke the audit role from the user test15:

```
kesl-control --revoke-role audit test15
```

Starting and stopping the application

After installing Kaspersky Endpoint Security to a device, the application is started automatically. By default, the application then starts automatically when the operating system is booted (at the default level of execution for each operating system).

By default, when Kaspersky Endpoint Security is started, the following functional components of the application are started automatically:

- 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 are not resumed automatically after the application is restarted.

Starting and stopping the application using the Web Console

To start or stop the application remotely:

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 12.1 for Linux** 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** web widget in the **Monitoring and reports / Dashboard** window.

Starting and stopping the application using the Administration Console

To start or stop the application on a client device:

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 12.1 for Linux**.
6. Do one of the following:

   - To run the application, click the  button to the right of the list of Kaspersky applications or select **Start** in the application context menu.
   - To stop the application, click the  button to the right of the list of Kaspersky applications or select **Stop** in the application context menu.

Starting and stopping 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.

Starting, restarting, and stopping Kaspersky Endpoint Security

To start the application, run the following command:

```
systemctl start kesl
```

To stop the application, run the following command:

```
systemctl stop kesl
```

To restart the application, run the following command:

```
systemctl restart kesl
```

Monitoring the status of Kaspersky Endpoint Security

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.

To export application settings, run the following command:

```
systemctl status kesl
```

Viewing the protection status of a device and application settings

You can view information about the protection status of a device, as well as the status of Kaspersky Endpoint Security and its components on the device.

You can get information about the protection status of a device in the following ways:

- In the Web Console or in the Administration Console, using the statuses of the client devices (*OK*, *Critical*, *Warning*). The device on which Kaspersky Security Center Network Agent is installed is a client device for Kaspersky Security Center. The status of a client device can change to *Critical* or *Warning* for the following reasons:

  - In accordance with the rules defined in Kaspersky Security Center. For example, the status changes if a security application is not installed on the device, a virus scan has not been performed in a long time, application databases are outdated, the license has expired, or the application is unstable. For more details on the reasons for changing statuses and configuring conditions for assigning statuses, refer to the Kaspersky Security Center Help system.

  - Kaspersky Security Center receives the device status from the managed application, i.e., from Kaspersky Endpoint Security.

    Receiving device status from a managed application must be enabled in Kaspersky Security Center in the lists of conditions for assigning the *Critical* and *Warning* statuses. Conditions for assigning device statuses are configured in the properties window of an administration group.

  For more details on client device statuses, refer to the Kaspersky Security Center Help system.

- In the Web Console or in the Administration Console, using the statuses of functional components of Kaspersky Endpoint Security on the device. In the properties of Kaspersky Endpoint Security installed on the device, a list of the functional components of the application is displayed. For each component, its status is displayed.

- In the command line, using the command `kesl-control --app-info`. The command displays information about the operation of the application and the status of functional components and tasks of the application.

Viewing the protection status of a device in the Web Console

To view the protection status of a 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 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. In the list, find the device for which you want to view information and click the device name.

4. In the properties window of the managed device that opens, 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.
- **Viruses detected** represents a total number 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.

Viewing the protection status of a device in the Administration Console

To view 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.

Viewing information about the operation of an application in the Web Console

To view information about the application operation 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 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. In the list, find the device for which you want to view information and click the device name.

4. This opens a managed device properties window; in that window, go to the **Applications** tab.

5. In the list of Kaspersky applications installed on the device, click the name of the **Kaspersky Endpoint Security 12.1 for Linux** application.

   The application properties window opens.

The **Kaspersky Endpoint Security 12.1 for Linux** window displays the following information about Kaspersky Endpoint Security:

- The **General** tab in the **Information** section displays general information about the installed application:
  - **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** is the 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**: status of File Threat Protection on the device, such as *Running* or *Paused*.
  - Under **Installed updates**, you can find information about application module 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.
- On the **General** tab, the **Licenses** section contains information about license keys added to the application and the licenses corresponding to these keys.
- On the **General** tab, the **Components** section contains a list of functional components of the application. The status (for example, *Stopped, Suspended, Not Installed*) and version of each component is displayed.

  In the **Light Agent mode for protecting virtual environments** line, you can see information about the application usage mode:

- The *Running* status means that the application is being used in Light Agent mode.
- The *Not installed* status means that the application is being used in Standard mode.

- The **Events** tab displays a list of application events on the device.
- The **Event settings** section displays the types of events that the application stores in event storage and how long they are stored.
- On **Application settings** tab, in the **Detection and Response** section, you can manage the network isolation of the device.

Viewing information about the operation of an application in the Administration Console

To view information about the application operation in the Kaspersky Security Center 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 12.1 for Linux** 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 **Kaspersky Endpoint Security 12.1 for Linux settings** window opens.

The **Kaspersky Endpoint Security 12.1 for Linux settings** window displays the following information about Kaspersky Endpoint Security:

- The **General** section contains general information about the installed application:
  - **Version number**: the version number of the application.
  - **Installed** — Date and time when the application was installed on the device.
  - **Current status**: status of File Threat Protection on the device, such as *Running* or *Paused*.
  - **Last software update**: date and time when Kaspersky Endpoint Security software modules were last updated.
  - **Installed updates**: list of software modules for which updates are installed.
  - **Application databases**: date and time when the application database updates were released.
- The **Components** section contains a list of standard application components. The status (for example, *Stopped, Suspended, Not Installed*) and version of each component is displayed.

In the **Light Agent mode for protecting virtual environments** line, you can see information about the application usage mode:

- The *Running* status means that the application is being used in Light Agent mode.
- The *Not installed* status means that the application is being used in Standard mode.

- The **License keys** section contains information about the active and reserve license keys:
  - **Serial number** – unique alphanumeric sequence.
  - **Status** – The status of the license key, e.g. active or reserve.
  - **Type**: type of license (commercial or trial).
  - **License validity period** — Number of days during which you can use the application activated with 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 **Event settings** section displays the types of events that the application stores in event storage and how long they are stored.
- The **Advanced** section contains information about the application administration plug-in.

Viewing information about the operation of an application in the command line

To view information about application, execute the following command:

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

where `--json`: output data in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

As a result of the command execution, the following information will be displayed in the console:

- **Name**. Application names.
- **Version**. Current application version.
- **Policy**. Information about whether a Kaspersky Security Center policy is applied on the device.
- **Application license information** Application license information or application license key status.
- **EDR Optimum license information**. Information about the license under which the Kaspersky Endpoint Detection and Response Optimum functionality is used, or the status of the EDR Optimum license key.

- **Subscription status**. Subscription status. This field is displayed if the application is started under a subscription.
- **Application license expiration date**. Date and time when the application license expires, in UTC.
- **EDR Optimum license expiration date**. Date and time when the license for using Kaspersky Endpoint Detection and Response Optimum functionality expires, in UTC.
- **MDR BLOB file status**. Status of the BLOB configuration file for integration with Kaspersky Managed Detection and Response.
- **MDR BLOB license expiration date**. Date and time when the Kaspersky Managed Detection and Response license expires, in UTC.
- **Backup state**. Backup state.
- **Backup space 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**. Information about whether the application databases were downloaded.
- **Using Kaspersky Security Network**. Information about using Kaspersky Security Network: `Extended KSN mode`, `Basic KSN mode` or `Disabled`.
- **Light Agent mode to protect virtual environments**. Information that the application is being used in Light Agent mode to protect virtual environments. If the application is being used in standard mode, the line is not displayed.
- **File disinfection and deletion disabled**. Information about the fact that an application operating mode is enabled in which files on disk are not disinfected and deleted, regardless of the settings configured in the policy properties.
- **Kaspersky Security Network infrastructure**. Information about the infrastructure solution used to work with Kaspersky reputation databases: `Kaspersky Security Network` or `Kaspersky Private Security Network`.
- **Integration with Kaspersky Managed Detection and Response**. Status of integration with Kaspersky Managed Detection and Response: `Enabled`, `Disabled`.
- **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.
- **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 (KATA) Integration**. Kaspersky Endpoint Detection and Response (KATA) integration status.
- **Actions after update**. Application update actions and the actions to be performed by the user.
- **Unstable application operation**. Information about application failure and dump file creation. This field is displayed if a failure occurred the last time the application was launched.

Application activation and license key management

Activation is the process of activating a license that allows you to use a fully functional version of the application until the license expires.

The process of activating Kaspersky Endpoint Security involves adding an active application license key.

If you are using the application under a license that does not include the Kaspersky Endpoint Detection and Response Optimum functionality, then to activate this functionality, you need to add an additional Kaspersky Endpoint Detection and Response Optimum Add-on license key ("EDR Optimum key").

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the application does not need to be activated separately. You activate Kaspersky Hybrid Cloud Security for Virtualization Light Agent; activation is performed on the Protection Server (a component of Kaspersky Hybrid Cloud Security for Virtualization Light Agent) by adding a license key to the SVM. To activate the functionality of Kaspersky Endpoint Detection and Response Optimum, you also need to add the EDR Optimum key to the SVM.

You can activate the application in one of the following ways:

- Remotely, using Kaspersky Security Center:
  - During installation of Kaspersky Endpoint Security. You can add a license key to the installation package. The application will be activated automatically after installation.
  - After installing Kaspersky Endpoint Security. You can add a license key to the application using the application activation task or by distributing the license key located on the Administration Server to the client devices.
- Using the command line:
  - During the initial configuration of Kaspersky Endpoint Security.
  - After installing Kaspersky Endpoint Security. You can add and remove license keys using administration commands.

You can also add a reserve key to the application. The reserve key becomes active when the license associated with the active key expires or when the active key is deleted. Availability of a reserve key allows you to avoid application functionality limitation when your license expires.

A reserve license key can be added only after adding an active license key.

You can view information about the license keys added to the device:

- Remotely in the Web Console or in the Administration Console. The properties of the application on the client device contain information about the active and reserve keys in the **License keys** section.
- In the command line using administration commands.

Viewing information about the license and the key in the command line

In the command line, using the `-L --query` command, you can view information about the active and reserve license keys added to the application, and about the license under which the application has been activated. If a separate key for activating the functionality of Kaspersky Endpoint Detection and Response Optimum has been added to the application, information about the active and reserve license keys of EDR Optimum and the EDR Optimum license is also displayed.

To view information about the license keys and license on the device, run the following command:

```
kesl-control -L --query [--json]
```

where `--json`: output data in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

As a result of the command execution, the following information will be displayed in the console:

- Information about the active application key, if a key has been added:
  - Date and time when the license for using the application expires.
  - Number of days before the end of the license term.
  - Information about the limitation of protection functions.
  - Information about the limitation of the function for updating application databases.
  - 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.
- Application reserve key information. Displayed if the application is being used in standard mode and a reserve key has been added. If the application is used in Light Agent mode to protect virtual environments, information about the reserve key is not displayed; the reserve key is added to the SVM.
  - Date and time when the license for using the application expires.
  - Number of days before the end of the license term.
  - Information about the limitation of protection functions.
  - Information about the limitation of the function for updating application databases.
  - 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.
    - Activation date.
- Information about the EDR Optimum active key, if a key has been added:
    - Date and time when the license for using Kaspersky Endpoint Detection and Response Optimum functionality expires.
    - Information about the limitation of the function for updating application databases.
    - 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.
- EDR Optimum reserve key information. Displayed if the application is being used in standard mode and a EDR Optimum reserve key has been added. If the application is used in Light Agent mode to protect virtual environments, information about the reserve key is not displayed; the reserve key is added to the SVM.
    - Date and time when the license for using Kaspersky Endpoint Detection and Response Optimum functionality expires.
    - Information about the limitation of the function for updating application databases.
    - 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.
    - Activation date.

License key management in the command line

To manage license keys on a device, you can use license key management commands.

You can use these commands to add application license keys as well as EDR Optimum license keys. You do not need to specify the type of the key in the commands.

The commands for managing license keys can be executed only if the application is used in standard mode. If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, commands for managing license keys finish with an error. You activate the application as part of Kaspersky Security for Virtualization Light Agent, and therefore do not need to activate the application separately.

To add an active license key to the application, run the following command:

```
kesl-control [-L] --add-active-key <path to key file / activation code>
```

where:

- `<path to the key file>` – 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>` – activation code.

To add a reserve license key to the application, run the following command:

```
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.

To remove an active application key, run the following command:

```
kesl-control [-L] --remove-active-key
```

To remove a reserve application key, run the following command:

```
kesl-control [-L] --remove-reserve-key
```

To remove an active EDR Optimum key, run the following command:

```
kesl-control [-L] --remove-active-key --edr-optimum
```

To remove a reserve EDR Optimum key, run the following command:

```
kesl-control [-L] --remove-reserve-key --edr-optimum
```

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, malware, and other types of threats appear worldwide on a daily basis. The application databases contain information about the threats and the ways to neutralize 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.

During the update process, the databases and application modules are downloaded and installed on your device.

You can obtain updates for databases and application modules from Kaspersky update servers, from the Administration Server repository, from local or network directories, and from other update sources.

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the directory on the SVM is used as an update source.

During an update, the application modules and databases on your device are compared with the up-to-date version 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.

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 in the general settings of the application.

Regardless of the update source, the update package is downloaded and the database and application module updates are installed on the device using the *Update* task.

An *Update* predefined task is created in the application. Using this task, you can perform scheduled and on-demand updates of databases and application modules and configure update settings.

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, 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.

If Kaspersky Endpoint Security is used in standard mode, in Kaspersky Security Center, you can use the *Update* group task that the Initial Configuration Wizard creates after installing the MMC administration plug-in or the Kaspersky Endpoint Security web administration plug-in.

You can also create update user tasks in the command line and in Kaspersky Security Center.

You can configure the following settings for updating databases and application modules:

- Select the source from which the application will receive updates, depending on the update scenario used.
- 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.
- Select the mode of downloading and installing application modules and application version updates: download and install, download only, or do not download.
- Configure the task run schedule for updates. By default, the application updates the databases once every 60 minutes.

Updating databases and modules

During an update, the following objects are downloaded and installed on your device:

- Application databases. Application databases include databases of malware signatures, a description of network attacks, databases of malicious and phishing web addresses, databases of banners, spam databases, and other data.

  If the database update on the device is interrupted or finishes with an error, the application continues to use the previously installed database version. If application databases were not installed before, the application continues functioning in "without databases" mode. Database and application module updates are still available.

  The databases are up to date if they were downloaded less than three days ago. By default, the application generates the *Databases are out of date* event (*BasesAreOutOfDate*) if the last installed database updates were published on the Kaspersky servers more than three but less than seven days ago. If the databases have not been updated for seven days, the application generates the *Databases are extremely out of date* (*BasesAreTotallyOutOfDate*) event.

- 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.

  The application module can be installed regardless of the state of the application (started or stopped, managed by a Kaspersky Security Center policy) and the update schedule. Kaspersky Endpoint Security continues protecting your device during the application modules update procedure. During the update, application settings and the application log file are migrated to the new version of the application. After the update, Kaspersky Endpoint Security needs to be restarted.

  If the transfer of application settings fails for any reason, the application is set to the default values.

  Changes to the application settings made after the update is complete and before the application restarts are not saved.

  After updating version of the application using an autopatch, the mechanism for interacting with the operating system firewall changes: the rules are managed using the iptables and iptables-restore system utilities.

  If the application does not work properly after the update, it automatically rolls back to the previous version. It is recommended to contact Kaspersky Technical Support.

Sources and scenarios for updates

An *update source* is a resource that contains updates for Kaspersky Endpoint Security databases and application modules. Update sources can be FTP, HTTP, or HTTPS servers (such as Kaspersky update servers), as well as local or network directories mounted by the user.

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the databases on the protected virtual machines are updated from the directory on the SVM.

The main application update sources are Kaspersky update servers. You can specify other update sources in the *Update* task settings. If an update cannot be performed from an update source, Kaspersky Endpoint Security switches to the next update source.

Kaspersky Endpoint Security supports the following scenarios for updating databases and application modules:

- 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.
- Centralized update 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.

     If you manage the application using Kaspersky Security Center Cloud Console, you can use the repositories of the distribution points (devices with Network Agent installed) as the repository. For more details about distribution points, refer to Kaspersky Security Center Help.

  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 the Kaspersky Security Center Administration Server as the update source.

- Updating from a local or network directory (SMB/NFS) mounted by a user, or from an FTP, HTTP, or HTTPS server. You can specify a custom update source in *Update* task settings.

Updating application databases and modules in the Web Console

The procedure for updating Kaspersky Endpoint Security databases and application modules depends on the application usage mode. This section describes the procedure for updating the application in standard mode. If the application is used in Light Agent mode to protect virtual environments, the databases and application modules cannot be updated using the tasks created in Kaspersky Security Center. Updates are performed using a local predefined task.

In the Web Console, you can update databases and application modules using the *Update* task. You can use the automatically created *Update* group task, as well as create user tasks for updating.

To configure update settings in the Web Console:

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

   The list of tasks opens.

2. Do one of the following:

- If you want to edit the settings of a task that is run on all devices included in a specific administration group, click the link in the **Current path** field in the upper part of the window and select the administration group in the window that opens.

  The list displays only tasks configured for the selected administration group.

- If you want to edit the settings of a task that is run on one or multiple devices (a task for a set of devices), click the link in the **Current path** field in the upper part of the window and select the top node with the name of the Administration Server in the window that opens.

  The list displays all tasks created on the Administration Server.

3. In the list of tasks, select the required **Update** task and open the task properties window by clicking the link in the task name.

4. In the task properties window, select **Application settings** tab. Select the **Update sources** section in the list on the left.

5. Select the update source from which the application will receive updates for databases and modules, depending on the update scenario used.

   If you are managing the application using the Web Console, the list of update sources contains Kaspersky update servers and the Kaspersky Security Center Administration Server. If you are managing the application using Kaspersky Security Center Cloud Console, the list of update sources contains Kaspersky update servers and distribution points (for more details about distribution points, refer to the Kaspersky Security Center Help system). You can add other update sources to the list.

   You can create a list of update sources by selecting the **Other sources on the local or global network** option. 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.

6. Go to the **Settings** section and configure other update settings.

7. Select the **Schedule** tab and configure the schedule for running the update 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 system.

8. Click the **Save** button to save the changes made.

The task will start according to the configured schedule. You can also run the task manually.

Update sources for the Update task section

Setting	Description
Update source	In this section, you can select the update source: • **Kaspersky update servers**, where database updates for Kaspersky applications are published (default value). • **Kaspersky Security Center** – Kaspersky Security Center Administration Server (this option is available only for the Web Console). • **Distribution Points** (this option is available only for the Kaspersky Security Center Cloud Console). • **Other sources on the local or global network** – HTTP, HTTPS, or FTP servers or directories on local network servers.

Use Kaspersky update servers if other update sources are not available	The check box enables or disables usage Kaspersky update servers as the update source, if the selected update sources are not available. This checkbox is available if the **Other sources on the local or global network** or **Kaspersky Security Center** option is selected in the **Update sources** block. The check box is selected by default.
Custom update sources	This table contains a list of custom sources of database updates. During the update process, the application accesses update sources in the order they appear in the table. The table contains the following columns: • **Update source** is HTTP, HTTPS, or FTP servers or directories on local network servers. • The toggle switch indicates whether the source is used in the task (**Enabled** or **Disabled**). You can turn the toggle switch in the table on or off, as well as select or clear the **Use this source** check box in the **Update source** window, which opens by clicking the link with the source name. This table is available if the **Other sources on the local or global network** option is selected. The table is empty by default. You can add, edit, delete, move up, or move down update sources in the table. Clicking the **Move down** button moves the selected item down in the table. This button is available if only one item is selected in the table. Clicking the **Move up** button moves the selected item up in the table. This button is available if only one item is selected in the table. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Update task settings section

Setting	Description
Maximum time to wait for a 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.

	Available 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 the mode for updating application databases: • **Do not download** updates. If this list item is selected, the application cannot be updated. • **Download only** update files, but do not install them on client devices (default value). • **Download and install** updates to client devices. After updates are installed, the application will restart automatically. This feature is not supported in the KESL container.

Updating application databases and modules in the Administration Console

The procedure for updating Kaspersky Endpoint Security databases and application modules depends on the application usage mode. This section describes the procedure for updating the application in standard mode. If the application is used in Light Agent mode to protect virtual environments, the databases and application modules cannot be updated using the tasks created in Kaspersky Security Center. Updates are performed using a local predefined task.

In the Administration Console, you can update databases and application modules using the *Update* task. You can use the automatically created *Update* group task, as well as create user tasks for updating.

To configure update settings 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 the required **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. 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 Kaspersky update servers and the Kaspersky Security Center Administration Server. You can add other update sources to the list.

You can create a list of update sources by selecting the **Other sources on the local or global network** option. 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** section and configure the schedule for running the update 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 system.

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.

Update sources for the Update task section

Setting	Description
Update source	In this section, you can select 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 on the local or global network** – HTTP, HTTPS, or FTP servers or directories on local network servers.
Use Kaspersky update servers if other update sources are not available	The check box enables or disables usage Kaspersky update servers as the update source, if the selected update sources are not available. This checkbox is available if the **Other sources on the local or global network** or **Kaspersky Security Center** option is selected in the **Update sources** block. The check box is selected by default.
Custom update sources	This table contains a list of custom sources of database updates. 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** – HTTP, HTTPS, or FTP servers or directories on local network servers. • **Status** indicates if the 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. This table is available if the **Other sources on the local or global network** option is selected. You can add, edit, delete, move up, or move down update sources in the table. Clicking the **Move down** button moves the selected item down in the table. This button is available if only one item is selected in the table.

	Clicking the **Move up** button moves the selected item up in the table. This button is available if only one item is selected in the table. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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. The table is empty by default.

Update task settings section

Setting	Description
Maximum time to wait for a 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. Available 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 the mode for updating application databases: • **Do not download** updates. If this list item is selected, the application cannot be updated. • **Download only** update files, but do not install them on client devices (default value). • **Download and install** updates to client devices. After updates are installed, the application will restart automatically. This feature is not supported in the KESL container.

Updating application databases and modules in the command line

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, 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.

On the command line, you can update databases and application modules in the following ways:

- Using the *Update* predefined task. You can manually start, stop, pause, or resume this task and configure the task run schedule. You can configure scan settings by editing the settings of this task.
- Using user tasks for updating (tasks of the *Update* type). You can manually start user tasks and configure the task schedule.

Update task settings

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 `[CustomSources.item_#]` section. 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.
`UseKLServersWhenUnavailable`	The application's access to Kaspersky update servers if all custom update sources are unavailable.	`Yes` (default value) — The application will connect to Kaspersky update servers if all custom update sources are unavailable. `No` — The application will not connect to Kaspersky update servers if all custom update sources are unavailable.
`ApplicationUpdateMode`	Application update download and installation mode.	`Disabled` — Do not download or install application updates. `DownloadOnly` (default value) — Download application updates, but do not install them. `DownloadAndInstall` — Automatically download and install application updates. After updates are installed, the application will restart automatically.
`ConnectionTimeout`	Response timeout (in	You can use only integers within the range

	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.	from 0 to 120. Default value: 10.
The **[CustomSources.item_#]** section contains the following settings:		
`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.
`Enabled`	Use of the update source specified in the `URL` setting. To run the task, at least one update source needs to be enabled.	`Yes` – the application uses the update source. `No` – The app doesn't use the update source. The default value is not defined.

Updating using 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 database updates 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 the Kaspersky Knowledge Base.

3. Configure application database and module updates from the specified shared directory to the remaining devices on the organization's LAN.

   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.

4. In the table of update sources, click the **Add** button and specify the path to the shared directory.

   The source address must match the address indicated in the Kaspersky Update Utility settings.

5. Select the **Use this source** check box and click **OK**.

6. In the table, set the order of the update sources using the **Up** and **Down** buttons.

7. Save the changes to the task settings.

Rolling back application database and module updates

If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, the task cannot be used to rollback database updates.

After the application databases are updated for the first time, the rollback of the application databases to their previous versions becomes available.

Every time a user starts the update process, Kaspersky Endpoint Security creates a backup copy of the current application databases. This allows you to roll back the application databases to a previous version if needed.

Rolling back the last database update may be useful, for example, if the new application database version contains invalid signatures, which causes Kaspersky Endpoint Security to block safe applications.

In the command line, to roll back updates, you can run the *Rollback* predefined task or create and run user tasks for rolling back updates (tasks of the *Rollback* type).

In Kaspersky Security Center, you can create rollback tasks for administration groups or for individual devices using the Web Console or the Administration Console.

The *rollback* task does not have any settings.

File Threat Protection.

File Threat Protection component prevents infection of the device file system. The component is enabled automatically with the default settings when Kaspersky Endpoint Security starts. It resides in the device operating memory and scans all files that are opened, saved, and launched in real time.

Upon detecting malware, Kaspersky Endpoint Security may remove the infected file and terminate the malware process started from this file.

The operation of the component is affected by the file operation interception mode, which you can select in the general settings of the application. By default, access to the file is blocked for the duration of the scan.

If File Threat Protection is enabled and Container monitoring is enabled, the application also scans all namespaces and containers on all supported operating systems.

You can enable or disable File Threat Protection, and also configure the protection settings:

- Select the file scan mode (when opened, or when opened and modified).
- Enable or disable scanning of archives, mail databases, email messages in text format.
- Temporarily exclude files in text format from rescans.
- Limit the size of an object to be scanned and the duration of the object scan.
- Select the actions to be performed by the application on the infected objects.
- Configure the scan scopes. The application will scan objects in the specified area of the file system.
- Configure exclusions of objects from scans. *Scan exclusion* is a set of conditions. When these conditions are met, the application does not scan the objects for viruses and other malware. You can exclude from scans:
  - Objects by name or mask
  - Objects by the name of the threats detected in them
  - Files and directories in specified areas of the file system
  - Processes and files being modified by the specified process
- Configure the use of the heuristic analyzer and iChecker technology during a scan.
- Enable or disable the logging of information about scanned non-infected objects, about scanning objects in archives, and about unprocessed objects.

To optimize the File Threat Protection component, you can exclude from scans any files being 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.

Configuring File Threat Protection in the Web Console

In the Web Console, you can manage File Threat Protection in the policy properties (**Application Settings** → **Essential Threat Protection**→ **File Threat Protection**).

File Threat Protection component settings

Setting	Description
File Threat Protection enabled / disabled	This toggle switch enables or disables File Threat Protection component on all managed devices. The check toggle button is switched on 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.
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Block** access to the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Block** access to the object (default value).
Scan scopes	Clicking the **Configure scan scopes** link opens the **Protection scopes** window.
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 enabling and configuring the **Skip file that is scanned for longer than (sec)** and **Skip file larger than (MB)** settings. If the check box is cleared, the application does not scan the 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 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 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 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 text files	Temporary exclusion of files in text format from scans. If the checkbox is selected, the application does not scan text files if they are reused by the same process for 10 minutes after the most recent scan. This setting makes it possible to optimize scans of application logs. If the check box is cleared, the application will scan text files. 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. Available values: `0`–`9999`. If the value is set to `0`, the scan time is unlimited. The default value is `60`.
Skip file larger than (MB)	In this field, you can specify the maximum size of a file to scan, in megabytes. Available values: `0`–`999999`. If the value is set to `0`, the application scans files of any size. The default value is `0`.
Log clean objects	This check box enables or disables logging of the *ObjectProcessed* event. If this check box is selected, the application logs the *ObjectProcessed* event for all scanned objects. If the check box is cleared, the application does not log the event. This check box is cleared by default.
Log unprocessed objects	This check box enables or disables logging of the *ObjectNotProcessed* event if a file cannot be processed during scan. If this check box is selected, the application logs the *ObjectNotProcessed* event. If the check box is cleared, the application does not log the event. This check box is cleared by default.
Log packed	This check box enables or disables logging of the *PackedObjectDetected* event for all

objects	packed objects that are detected. If this check box is selected, the application logs the *PackedObjectDetected* event. If the check box is cleared, the application does not log the event. 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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during an object scan. The 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 value) is the optimal level recommended by Kaspersky experts. It ensures an optimal combination of quality of protection and impact on the performance of protected servers.

Protection 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 protection scope that includes all shared directories.

Protection 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.

Add protection scope window

In this window, you can add and configure protection scopes.

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 operation. If this check box is cleared, the application does not process this protection scope during operation. You can later include this scope in the component settings by selecting the check box. The check box is selected by default.
File system, access protocol, and path	You can select the type of file system in the drop-down list: • **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.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Shared** or **Mounted** type is selected in the drop-down list of file systems.
Path	The entry field for specifying the path to the directory that you want to include in the protection scope. You can use masks and tags to specify the path. You can use special tags to specify a container or image: • `[container-id:<identifier>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<identifier>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags. 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:<identifier>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<identifier>]/<path to local directory>` • `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>` You can use masks (`?` and `*` characters) in names and identifiers.

	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. The **/** path is specified by default – the application scans all directories of the local file system. This field is available if the **Local** type is selected in the drop-down list of file systems. 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.
Name of shared resource	The field for entering the name of the file system shared resource where the directories that you want to add to the protection scope are located. The field is available if the **Mounted** type is selected in the File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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 Web Console, you can configure File Threat Protection exclusions in the policy properties (**Application Settings** → **Essential Threat Protection**→ **File Threat Protection exclusions**).

Settings of protection exclusions

Setting	Description
Exclusion scopes	Clicking the **Configure exclusions** link opens the **Exclusion scopes** window. In this window, you can define the list of protection exclusions.
Exclusions by mask	Clicking the **Configure exclusions by mask** link 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	Clicking the **Configure exclusions by threat name** link 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	Clicking the **Configure exclusions by process** link opens the **Exclusions by process** window. In this window, you can exclude the activity of processes.

Exclusion scopes window

This table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

Add exclusion scope window

In this window, you can add and configure 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	This check box enables or disables the exclusion of the scope when the application is running. If the check box is selected, the application excludes this scope from scan or protection during its operation. If the check box is cleared, the application includes this scope in scan or protection during its operation. You can later exclude this scope from scan or protection by selecting the check box. The check box is selected by default.
File system, access protocol, and path	In this drop-down list, you can select the type of file system where the directories that you want to add to scan exclusions are located: • **Local**, for local directories. • **Mounted**, for remote directories mounted on the device. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Mounted** type is selected in the drop-down list of file systems.
Path	Entry field for the path to the directory that you want to add to the exclusion scope. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>], [container-name:<name>], [image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. The **/** path is specified by default. The application excludes all directories of the local file system from scan. This field is available if the **Local** type is selected in the drop-down list of file systems.
Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Exclusions by process window

The table contains the exclusion scopes for exclusion by process 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 table 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
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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

Trusted process window

In this window, you can add and configure exclusion scopes for exclusion by process.

Exclusion scope settings

Setting	Description
Process-based exclusion scope name	Field for entering the Process-based exclusion scope name. This name will be displayed in a table in the **Exclusions by process** window. The entry field must not be blank.
Use / Do not use this exclusion	This toggle switch enables or disables this scan scope exclusion. The check toggle button is switched on by default.

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.
Path to excluded process	Full path to the process you want to exclude from scans.
File system, access protocol, and path	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. • **Mounted** – mounted directories. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. The **Access protocol** drop-down list is available if the **Mounted** type is selected in the drop-down list of file systems.
Path	In the input field, you can enter the path to the directory that you want to add to the exclusion scope. You can use masks to specify the path. 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. To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk). The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself. You can use a single ? character to represent any one character in the file or directory name. This field is available if the **Local** type is selected in the drop-down list of file systems.

Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
Masks	The list contains name masks of the objects that the application excludes from scan. Masks are applied to objects only inside the directory indicated in the **File system, access protocol, and path** block. By default the list contains the * mask (all objects). You can add, edit, or delete masks. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans. 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).

Configuring File Threat Protection in the Administration Console

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. The 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.
Action on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Action 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. The 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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

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.

	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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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.
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 checkbox is selected, Kaspersky Endpoint Security does not scan text files if they are reused by the same process for 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.
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. Available 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. Available 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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.

Action 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
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Block** access to the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Block** access to the object (default value).

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 table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

<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. The 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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

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.

To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk).

The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself.

You can use a single ? character to represent any one character in the file or directory name.

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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Exclusions by process window

The table contains the exclusion scopes for exclusion by process 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 table 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
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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected 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	Full path to the process you want to exclude from scans.

process	
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. The 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.

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.

To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk).

The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself.

You can use a single ? character to represent any one character in the file or directory name.

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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans. 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).

Configuring File Threat Protection in the command line

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.

File Threat Protection task settings

The table describes all available values and default values of all the settings that you can specify for the File Threat Protection task.

File Threat Protection 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`—Scan archives. If the `FirstAction=Recommended` value is specified, 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.	`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.

	If the value of this setting is `SkipPlainTextFiles=Yes`, the application does not scan text files if they are reused by the same process for 10 minutes after the most recent scan. This setting makes it possible to optimize scans of application logs.	
`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 – 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 – 9999 0 — The object scan time is unlimited. Default value: 60.
`FirstAction`	Selection of the first action to be performed by the application on the infected objects.	`Disinfect` — The application tries to disinfect an object and save a copy of it to Backup. If disinfection fails (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application leaves the object unchanged. If the first action is `Disinfect`, it is recommended to specify a second action using the `SecondAction` setting. `Remove` — The application removes the infected object after creating a backup copy of it. `Recommended` (perform recommended action) — The application automatically selects and performs an action on the object based on information about the threat detected in the object. For example Kaspersky Endpoint Security immediately removes Trojans since they do not incorporate themselves into other files and therefore they do not need to be disinfected. `Block` – The application blocks access to an infected object. Information about the infected object is logged. Default value: `Recommended`.
`SecondAction`	Selection of the second action to be performed by the application on the infected objects. The application performs the second action if the first action fails.	The possible values of the `SecondAction` setting are the same as those of the `FirstAction` setting.

		If `Block` or `Remove` is selected as the first action, the second action does not need t be specified. It is recommended to specify two actions in all other cases. If you have n specified a second action, the application applies `Block` as the second action. Default value: `Block`.
`UseExcludeMasks`	Enables scan exclusions for the objects specified by the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scar `No` (default value) — Do not exclude object specified by the `ExcludeMasks.item_#` setting from scans.

`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 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 scans. `No` (default value) — Do not exclude object containing the threats specified by the `ExcludeThreats.item_#` setting from scans.

`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 collect 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-infecte objects. `No` (default value) — Do not log informatio 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 informatio about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocesse objects. `No` (default value) — Do not log informatio 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. 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 leve 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 applies only to the File Threat Protection task.	`SmartCheck` (default value) — Scan a file 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 operatio and modifies it, the application scans the object again only when the process closes it for the last time. `OpenAndModify` — Scan a file on attempt to open it, and scan it again on attempts t 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 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. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

		You can use masks (`?` and `*` characters) in names and identifiers. 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. `Shared:NFS` — Scan the device file syster resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samb 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 th Samba and NFS protocols. `AllShared` – Scan all the device file syste resources that are accessible via the Samb and NFS protocols. `<file system type>` — Scan all the resources of the specified device file system.
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan	The default value is not defined.

	exclusion scope, which contains additional information about the exclusion scope.	
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specifie 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 directory>` — Exclud objects in the specified directory (includin subdirectories) from scans. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

		You can use masks (`?` and `*` characters) in names and identifiers. 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. `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 th Samba and NFS protocols from scan. `<file system type>` — Exclude all the resources of the specified device file syste from scans.
The **[ExcludedForProgram.item_#]** section contains the following settings:		
`ProgramPath`	Path to excluded process.	`< full path to process >` – Do not sca the process in the indicated local directory
`ApplyToDescendants`	Exclude child processes of the excluded process specified by the `ProgramPath` setting from scans.	`Yes` – exclude the specified process and a 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 specifie scope. `No` — Do not exclude the specified scope.
`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 directory>` — Exclud objects in the specified directory from sca You can use masks to specify the path. 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. `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 Samb 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 th 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 all the resources of the specified device file syste from scans.

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 the File Threat Protection task settings (*File_Threat_Protection*, ID:1) to a configuration file using the command:

   ```
   kesl-control --get-settings 1 --file <full path to 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_#` – file name mask for files to be excluded from the scan scope. 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. Execute the command:

   ```
   kesl-control --set-settings 1 --file <full path to configuration file> [--json]
   ```

   Specify the `--json` key if you are importing settings from a configuration file in JSON format. If the key 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.

Special considerations for scanning symbolic links and hard links

Kaspersky Endpoint Security lets you scan symbolic links and hard links to files.

Scanning symbolic links

The application scans symbolic links only if the file referenced by the symbolic link is within the scan scope of the File Threat Protection component.

If the file referenced by the symbolic link is not within the scan scope of the File Threat Protection component, the application does not scan this file. However, if the file contains malicious code, the security of the device is at risk.

Scanning hard links

When processing a file with more than one hard link, the application chooses an action depending on the specified action on objects:

- If the **Perform recommended action** option is selected, the application automatically selects and performs an action on an object based on data about the danger level of the threat detected in the object and the possibility of disinfecting it.
- If the **Remove** action is selected, the application removes the hard link being processed. The remaining hard links to this file will not be processed.
- If the **Disinfect** action is selected, the application disinfects the source file. If disinfection fails, the application deletes the hard link and creates in its place a copy of the source file with the name of the deleted hard link.

When you restore a file with a hard link from the Backup storage, the application creates a copy of the source file with the name of the hard link that was moved to the Backup storage. Connections with the remaining hard links to the source file will not be restored.

Malware Scan

Malware Scan is a one-time full or custom file scan on the device performed on demand. Kaspersky Endpoint Security can carry out multiple Malware Scan tasks at the same time.

A *Malware Scan (Scan_My_Computer)* predefined task is created in the application. 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.

In Kaspersky Security Center, the Kaspersky Security Center Initial Configuration Wizard automatically creates a Malware Scan group task after installing the MMC administration plug-in or the Kaspersky Endpoint Security web administration plug-in.

During a full disk scan, the processor is busy. It is recommended to run the full scan task when the business is idle.

You can configure the settings of automatically created tasks in Kaspersky Security Center and in the command line, and also create Malware Scan user tasks.

Upon detecting malware, Kaspersky Endpoint Security may remove the infected file and terminate the malware process started from this file.

If during execution of the malware scan task the application was restarted by a control service or manually by the user, the task will be stopped. The application logs the *OnDemandTaskInterrupted* event.

You can run Malware Scan tasks and configure scan settings:

- Select operating system objects to scan: files, archives, boot sectors, process memory and kernel memory, startup objects.
- Limit the size of an object to be scanned and the duration of the object scan.
- Select the actions to be performed by the application on the infected objects.
- Configure exclusions of objects from scans:
  - by name or mask
  - by the name of the threats detected in the objects
- Enable or disable global exclusions and File Threat Protection exclusions when scanning.
- Enable the logging of information about scanned non-infected objects, about scanning objects in archives, and about unprocessed objects.
- Configure the use of the heuristic analyzer and iChecker technology during a scan.
- Limit the set of devices whose boot sectors need to be scanned.
- Configure scan scopes and scan exclusion scopes.

Malware Scan in the Web Console

In the Web 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 configure scan settings by editing the settings of Malware Scan tasks.

Malware Scan task 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. The 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 unchecked. The 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. Available 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. Available 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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Skip** the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup.

	• **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Skip** the object (default value).
Scan scopes	The table that contains the scopes scanned by the task. By default, the table contains one scan scope that includes all directories of the local file system. You can add, configure, delete, move up, or move down scan scopes 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. Clicking the scan scope name opens the **<Scan scope name>** window. In this window, you can modify the settings of the selected scan scope. Clicking the **Add** button opens the **<New scan scope>** window. In this window, you can define a new scan scope.

Add scan scope window

In this window, you can add and configure scan scopes.

Scan scope settings

Setting	Description

Scope name	Field for entering the scan scope name. This name is displayed in the **Scan scopes** table in the **Scan settings** section. 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. The check box is selected by default.
File system, access protocol, and path	You can select the type of file system in the drop-down list: • **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.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Shared** or **Mounted** type is selected in the drop-down list of file systems.
Path	This is the entry field for specifying the path to the directory that you want to include in the scan scope. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

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.

	The **/** path is specified by default – the application scans all directories of the local file system. This field is available if the **Local** type is selected in the drop-down list of file systems. 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.
Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Scan scopes section

You can configure scan scope settings for the Malware Scan task. The application allows you to scan files, boot sectors, client device memory, and startup objects.

Malware Scan scope task 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. The 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 client device memory scan. If the checkbox is selected, the application scans kernel memory and running processes. If the checkbox 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	Clicking the **Configure device masks** link opens the **Scan scopes** window, where you can specify the devices whose boot sectors will be scanned.

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.

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.

Exclusion scopes section

In the **Exclusion scopes** section for the Malware Scan task, you can configure exclusion scopes, exclusions by mask and threat name, as well as the use of global exclusions and File Threat Protection exclusions when the task is running.

Settings of scan exclusions

Setting	Description
Configure exclusion scopes	Clicking the **Configure exclusions** link opens the **Exclusion scopes** window. In this window, you can define the list of scan exclusions.
Configure exclusions by mask	Clicking the **Configure exclusions by mask** link opens the **Exclusions by mask** window. In this window, you can configure the exclusion of objects from scans by name mask.
Configure exclusions by threat name	Clicking the **Configure exclusions by threat name** link 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.

	The 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. The check box is selected by default.

Exclusion scopes window

This table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

Add exclusion scope window

In this window, you can add and configure 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	This check box enables or disables the exclusion of the scope when the application is running. If the check box is selected, the application excludes this scope from scan or protection during its operation.

	If the check box is cleared, the application includes this scope in scan or protection during its operation. You can later exclude this scope from scan or protection by selecting the check box. The check box is selected by default.
File system, access protocol, and path	In this drop-down list, you can select the type of file system where the directories that you want to add to scan exclusions are located: • **Local**, for local directories. • **Mounted**, for remote directories mounted on the device. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Mounted** type is selected in the drop-down list of file systems.
Path	Entry field for the path to the directory that you want to add to the exclusion scope. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. The **/** path is specified by default. The application excludes all directories of the local file system from scan. This field is available if the **Local** type is selected in the drop-down list of file systems.
Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Malware Scan in the Administration Console

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 configure scan settings by editing the settings of Malware Scan tasks.

In the **Settings** section of the properties of the Malware Scan task, you can configure 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.
Action on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Action on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

In the **Exclusions** section of the Malware Scan task properties, you can also configure exclusion scopes or exclusions by mask and by the 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. The check box is selected by default.
File system, access	The settings block lets you set the scan scope. You can select the file system type in the drop-down list of file systems:

protocol, and path	• **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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>], [container-name:<name>], [image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

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.

	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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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. The 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 checkbox is selected, the application scans kernel memory and running processes. If the checkbox is cleared, the application does not scan kernels and running processes. This check box is cleared by default.
Scan startup	This check box enables or disables startup object scans.

objects	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. The 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. The 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.

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.

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. The 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 unchecked. The 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. Available 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. Available 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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.

Action 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
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Skip** the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup.

	• **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Skip** the object (default value).

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 table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

<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. The 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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. 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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Malware Scan in the command line

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 run schedule. You can configure scan settings by editing the settings of this task.
- Using Malware Scan user tasks (tasks of the *ODS* type). You can manually start, stop, pause, or resume user tasks and configure the task schedule.
- Using the command `kesl-control --scan-file`, you can perform a *custom scan* of the specified files and directories.

Malware Scan predefined task settings

The table describes all available values and the default values of all the settings that you can specify for the Malware Scan task.

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 memo 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 the `FirstAction=Recommended` value is specified, 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 – 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 – 9999 0 — The object scan time is unlimited. Default value: 0.
`FirstAction`	Selection of the first action to be performed by the application on the infected objects.	`Disinfect` — The application tries to disinfect an object and save a copy of it to Backup. If disinfection fails (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application leaves the object unchanged. If the first action is `Disinfect`, it is recommended to specify a second action using the `SecondAction` setting. `Remove` — The application removes the infected object after creating a backup copy of it. `Recommended` (perform recommended action) — The application automatically selects and performs an action on the object based on information about the threat detected in the object. For example Kaspersky Endpoint Security immediately removes Trojans since they do not incorporate themselves into other files and therefore they do not need to be disinfected.

		`Skip` — The application does not try to disinfect or delete infected objects. Information about the infected object is logged. Default value: `Recommended`.
`SecondAction`	Selection of the second action to be performed by the application on the infected objects. The application performs the second action if the first action fails.	The possible values of the `SecondAction` setting are the same as those of the `FirstAction` setting. If `Skip` or `Remove` is selected as the first action, the second action does not need t be specified. It is recommended to specify two actions in all other cases. If you have n specified the second action, the applicatic applies `Skip` as the second action. Default value: `Skip`.
`UseExcludeMasks`	Enables scan exclusions for the objects specified by the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scar `No` (default value) — Do not exclude object specified by the `ExcludeMasks.item_#` setting from scans.

`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 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 scans. `No` (default value) — Do not exclude object containing the threats specified by the `ExcludeThreats.item_#` setting from scans.

`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.
		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`

	For example, you may be using a utility to collect 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.	
`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-infecte objects. `No` (default value) — Do not log informatio 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 informatio about scanned objects within archives.
`ReportUnprocessedObjects`	Enables logging of information about objects that have not been processed for some reason.	`Yes` — Log information about unprocesse objects. `No` (default value) — Do not log informatio 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.	`Light` — The least thorough scan with minimum load on the system. `Medium` — A medium heuristic analysis leve with a balanced load on the system. `Deep` — The most thorough scan with maximum load on the system.

	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.	`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 matc the specified mask. Default value: `/**` – any set of characters 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_<item number>=*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 syster resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file systen resources that are accessible via the Samb 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 th Samba and NFS protocols. `AllShared` – Scan all the device file syste resources that are accessible via the Samb and NFS protocols. `<file system type>` — Scan all the resources of the specified device file system.
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 specifie 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>` — Exclud objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path.

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.

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 t 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/.

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 th Samba and NFS protocols from scan.

< file system type > — Exclude all the resources of the specified device file syste from scans.

Remote directories are excluded from scans 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 scans.

Custom scan of files and directories

You can perform a custom scan of the specified files and directories using the command `kesl-control --scan-file`.

A custom scan is performed with the settings stored in the predefined task *Scan_File* (ID: 3). You can configure settings for a custom scan of files by editing the settings of this task (see the table below).

To start a custom scan of the specified files and directories, execute the following command:

```
kesl-control --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 to be performed by the application on the infected objects. If you do not specify the `--action` key, the application performs the recommended action.

As a result of executing the command, a temporary file scan task is created, which is automatically deleted after completion. In this case, the scan results are output to the console.

The table describes all available values and the default values of all the settings that you can specify for the *Scan_File* task.

The `[ScanScope.item_ #]` and `[ExcludedFromScanScope.item_ #]` sections defined in the *Scan_File* task are not taken into account when performing the custom scan.

Scan_File 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	`Yes` (default value) — Scan archives. If the `FirstAction=Recommended` value is

	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.	specified, 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 – 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 – 9999 0 — The object scan time is unlimited. Default value: 0.
`FirstAction`	Selection of the first action to be performed by the application on the infected objects.	`Disinfect` — The application tries to disinfect an object and save a copy of it to Backup. If disinfection fails (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application leaves the object unchanged. If the first action is `Disinfect`, it is recommended to specify a second action using the `SecondAction` setting. `Remove` — The application removes the infected object after creating a backup copy of it. `Recommended` (perform recommended action) — The application automatically selects and performs an action on the object based on information about the threat detected in the object. For example Kaspersky Endpoint Security immediately removes Trojans since they do not incorporate themselves into other files and therefore they do not need to be disinfected.

		`Skip` — The application does not try to disinfect or delete infected objects. Information about the infected object is logged. Default value: `Recommended`.
`SecondAction`	Selection of the second action to be performed by the application on the infected objects. The application performs the second action if the first action fails.	The possible values of the `SecondAction` setting are the same as those of the `FirstAction` setting. If `Skip` or `Remove` is selected as the first action, the second action does not need t be specified. It is recommended to specify two actions in all other cases. If you have n specified the second action, the applicatic applies `Skip` as the second action. Default value: `Skip`.
`UseExcludeMasks`	Enables scan exclusions for the objects specified by the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scar `No` (default value) — Do not exclude object specified by the `ExcludeMasks.item_#` setting from scans.

`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 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 scans. `No` (default value) — Do not exclude object containing the threats specified by the `ExcludeThreats.item_#` setting from scans.

`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.
		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`

	For example, you may be using a utility to collect 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.	
`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.	`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.

	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.	`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 matc the specified mask. Default value: `/**` – any set of characters 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="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. 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. `Shared:NFS` — Scan the device file syster resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file system resources that are accessible via the Samb 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 th Samba and NFS protocols. `AllShared` – Scan all the device file syste resources that are accessible via the Samb and NFS protocols. `<file system type>` — Scan all the resources of the specified device file system.
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 specifie 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>` — Exclud objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path.

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.

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 t 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/.

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 th Samba and NFS protocols from scan.

< file system type > — Exclude all the resources of the specified device file syste from scans.

Remote directories are excluded from scans 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 scans.

Critical Areas Scan

When performing a critical areas scan, Kaspersky Endpoint Security can scan boot sectors, startup objects, process memory, and kernel memory.

Upon detecting malware, the application can remove the infected file and terminate the malware process started from this file.

You can start a critical areas scan and configure the settings of the scan:

- Select the operating system objects to be scanned. Scanning of boot sectors, process memory and kernel memory, startup objects and archives is enabled by default. By default, files are not scanned during the critical areas scan.
- Limit the size of an object to be scanned and the duration of the object scan.
- Select the actions to be performed by the application on the infected objects.
- Configure exclusions of objects from scans:
  - by name or mask
  - by the name of the threats detected in the objects
- Enable or disable global exclusions and File Threat Protection exclusions when scanning.
- Enable the logging of information about scanned non-infected objects, about scanning objects in archives, and about unprocessed objects.
- Configure the use of the heuristic analyzer and iChecker technology during a scan.
- Limit the set of devices whose boot sectors need to be scanned.
- Configure scan scopes and scan exclusion scopes.

Critical Areas Scan in the Web Console

In the Web 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 critical areas scan user tasks. You can configure the scan settings by editing the settings of the tasks.

Critical Areas Scan task 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.

	The 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 unchecked. The 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. Available 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. Available 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.
Notify about unprocessed files	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	This check box enables or disables scan of only new and modified since the last scan files.

technology	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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Skip** the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Skip** the object (default value).
Scan scopes	The table that contains the scopes scanned by the task. By default, the table contains one scan scope that includes all directories of the local file system. You can add, configure, delete, move up, or move down scan scopes 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.

Clicking the scan scope name opens the **<Scan scope name>** window. In this window, you can modify the settings of the selected scan scope.

Clicking the **Add** button opens the **<New scan scope>** window. In this window, you can define a new scan scope.

Add scan scope window

In this window, you can add and configure scan scopes.

Scan scope settings

Setting	Description
Scope name	Field for entering the scan scope name. This name is displayed in the **Scan scopes** table in the **Scan settings** section. 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. The check box is selected by default.
File system,	You can select the type of file system in the drop-down list:

access protocol, and path	• **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.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Shared** or **Mounted** type is selected in the drop-down list of file systems.
Path	This is the entry field for specifying the path to the directory that you want to include in the scan scope. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>], [container-name:<name>], [image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

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.

	The **/** path is specified by default – the application scans all directories of the local file system. This field is available if the **Local** type is selected in the drop-down list of file systems. 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.
Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Scan scopes section

Scan scope settings for the Critical area scan task

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 cleared 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. The check box is selected by default.
Scan kernel memory and running processes	This check box enables or disables client device memory scan. If the checkbox is selected, the application scans kernel memory and running processes. If the checkbox is cleared, the application does not scan kernel memory and running processes. The check box is selected 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. The check box is selected by default.
Devices to scan	Clicking the **Configure device masks** link opens the **Scan scopes** window, where you can specify the devices whose boot sectors will be scanned.

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.

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.

Exclusion scopes section

In the **Exclusion scopes** section for the Critical Areas Scan task, you can configure exclusion scopes, exclusions by mask and by threat name, as well as the use of global exclusions and File Threat Protection exclusions when the task is running.

Settings of scan exclusions

Setting	Description
Configure exclusion scopes	Clicking the **Configure exclusions** link opens the **Exclusion scopes** window. In this window, you can define the list of scan exclusions.
Configure exclusions by mask	Clicking the **Configure exclusions by mask** link opens the **Exclusions by mask** window. In this window, you can configure the exclusion of objects from scans by name mask.
Configure exclusions by threat name	Clicking the **Configure exclusions by threat name** link 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. The check box is selected by default.
Use File Threat	This check box enables or disables the use of configured File Threat Protection

Protection exclusions	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. The check box is selected by default.

Exclusion scopes window

This table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

Add exclusion scope window

In this window, you can add and configure 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	This check box enables or disables the exclusion of the scope when the application is running. If the check box is selected, the application excludes this scope from scan or protection during its operation. If the check box is cleared, the application includes this scope in scan or protection during its operation. You can later exclude this scope from scan or protection by selecting the check box.

	The check box is selected by default.
File system, access protocol, and path	In this drop-down list, you can select the type of file system where the directories that you want to add to scan exclusions are located: • **Local**, for local directories. • **Mounted**, for remote directories mounted on the device. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Mounted** type is selected in the drop-down list of file systems.
Path	Entry field for the path to the directory that you want to add to the exclusion scope. You can use masks and tags to specify the path.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. The **/** path is specified by default. The application excludes all directories of the local file system from scan. This field is available if the **Local** type is selected in the drop-down list of file systems.
Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Critical Areas Scan in the Administration Console

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 critical areas scan user tasks. You can configure the scan settings by editing the settings of the tasks.

In the **Settings** section of the properties of the Critical Areas Scan task, you can configure 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.
Action on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Action on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

In the **Exclusions** section of the Critical Areas Scan task properties, you can also configure exclusion scopes or exclusions by mask and by the 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. The check box is selected by default.
File system, access	The settings block lets you set the scan scope. You can select the file system type in the drop-down list of file systems:

protocol, and path	• **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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>], [container-name:<name>], [image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

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.

	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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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. The check box is selected by default.
Scan kernel memory and running processes	This check box enables or disables device memory scan. If the checkbox is selected, Kaspersky Endpoint Security scans kernel memory and running processes. If the checkbox is cleared, Kaspersky Endpoint Security does not scan kernel memory and running processes. The 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. The 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.
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. The 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. The 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.

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.

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. The 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 unchecked. The 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. Available 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. Available 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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.

Action 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
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Skip** the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup.

	• **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Skip** the object (default value).

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 table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

<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. The 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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk). The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself. You can use a single ? character to represent any one character in the file or directory name. 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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Critical Areas Scan in the command line

In the command line, you can perform a critical areas scan of the operating system of a protected device using the Critical Areas Scan predefined task (*Critical_Areas_Scan*).

You can manually start, stop, pause, or resume this task and configure the task run schedule. You can configure scan settings by editing the settings of this task.

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 memo 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 the `FirstAction=Recommended` value is specified, 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 – 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 – 9999 0 — The object scan time is unlimited. Default value: 0.
`FirstAction`	Selection of the first action to be performed by the application on the infected objects.	`Disinfect` — The application tries to disinfect an object and save a copy of it to Backup. If disinfection fails (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application leaves the object unchanged. If the first action is `Disinfect`, it is recommended to specify a second action using the `SecondAction` setting. `Remove` — The application removes the infected object after creating a backup copy of it. `Recommended` (perform recommended action) — The application automatically selects and performs an action on the object based on information about the threat detected in the object. For example Kaspersky Endpoint Security immediately removes Trojans since they do not incorporate themselves into other files and therefore they do not need to be disinfected. `Skip` — The application does not try to disinfect or delete infected objects. Information about the infected object is logged. Default value: `Recommended`.
`SecondAction`	Selection of the second action to be performed by the application on the infected objects. The application performs the second action if the first action fails.	The possible values of the `SecondAction` setting are the same as those of the `FirstAction` setting. If `Skip` or `Remove` is selected as the first action, the second action does not need to be specified. It is recommended to specify two actions in all other cases. If you have not specified the second action, the application applies `Skip` as the second action.

		Default value: `Skip`.
`UseExcludeMasks`	Enables scan exclusions for the objects specified by the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scar `No` (default value) — Do not exclude object specified by the `ExcludeMasks.item_#` setting from scans.

`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 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 scans. `No` (default value) — Do not exclude object containing the threats specified by the `ExcludeThreats.item_#` setting from scans.

`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 collect 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.	`AllObjects` – scan boot sectors of all devices.

	The setting value cannot be empty. At least one device name mask must be specified to run this task.	`<device name mask>` – Scan boot sectors of the devices whose names matc the specified mask. Default value: `/**` – any set of characters 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 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. `Shared:NFS` — Scan the device file syster resources that are accessible via the NFS protocol. `Shared:SMB` – Scan the device file syster resources that are accessible via the Samb 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 th Samba and NFS protocols. `AllShared` – Scan all the device file syste resources that are accessible via the Samb and NFS protocols. `<file system type>` — Scan all the resources of the specified device file system.
The **[ExcludedFromScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of the scan exclusion scope, which contains	The default value is not defined.

	additional information about the exclusion scope.	
`UseScanArea`	Excludes the specified scope from scans.	`Yes` (default value) — Exclude the specifie 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>` — Exclud objects in the specified directory from sca You can use masks to specify the path. 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. 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 t 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/`.

`<path to local directory>` — Exclud objects in the specified directory (including subdirectories) from scans. You can use masks to specify the path.

> 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.

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 t 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/`.

`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 th Samba and NFS protocols from scan.

`<file system type>` — Exclude all the resources of the specified device file syste from scans.

		Remote directories are excluded from scans 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 scans.

Removable Drives Scan

Kaspersky Endpoint Security can scan the following removable drives when they are connected to the protected device: CDs, DVDs, Blu-ray discs, flash drives (including USB modems), external hard drives, and floppy disks.

If the removable drives scan is enabled, Kaspersky Endpoint Security monitors the connection of removable drives to the protected device and, if a connected removable drive is detected, it scans the drive and its boot sectors for viruses and other malware.

By default, the application does not monitor for the connection of removable drives or scan these.

This feature is not supported in the KESL container.

Configuring Removable Drives Scan in the Web Console

In the Web Console, you can configure the settings for the removable drives scan in the policy properties (**Application Settings** → **Local Tasks** → **Removable Drives Scan**).

Removable Drives Scan component settings

Setting	Description
Removable Drives Scan enabled / disabled	This option enables or disables the scan of removable drives when they are connected to the user device. The toggle button is switched off 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. The following file formats are scanned on removable drives: 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, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **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.

	The following file formats are scanned on removable drives: 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, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **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.

Configuring Removable Drives Scan in the Administration Console

In the Administration Console, you can configure the settings for the removable drives scan in the policy properties (Application Settings → **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. The following file formats are scanned on removable drives: 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, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **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. The following file formats are scanned on removable drives: 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, jpeg, emf, ico, ov?, xl*, xlsb, pp*, md*, sldx, sldm, thmx. • **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.

Configuring Removable Drives Scan in the command line

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 stopped 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 change 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 drives when they are 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 drives (except 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 removable drives (except CD/DVD drives and Blu-ray discs).

		The following file formats are scanned on removable drives: 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, 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 drives when they are connected.
`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 drives: 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, 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

You can scan containers and images for malware in real time and on demand:

- The *Container Monitoring* component allows you to scan launched containers and namespaces in real time.
- You can use the *Container Scan* tasks to scan containers and images on demand.

Application supports integration with Docker container management system, CRI-O framework, and Podman and runc utilities is supported.

To use the Container Scan tasks, a license that includes this function is required.

Container monitoring

The Container Monitoring component is enabled by default. The application scans running containers and namespaces in real time.

For the Container Monitoring component to work, the File Threat Protection component must be enabled. The File Threat Protection settings are used when scanning containers and namespaces.

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`".

You can enable or disable the Container Monitoring component, and also configure the settings for scanning containers and namespaces in real time:

- Select the action that the application performs on a container when it detects an infected object.

  This setting is available when using the application under a license that supports this function.

- Configure the integration of Kaspersky Endpoint Security with the Docker container management system, CRI-O framework, and Podman and runc utilities.

Configuring container monitoring in the Web Console

In the Web Console, you can manage the operation of the *Container Monitoring* component in the policy properties (**Application settings** → **General settings** → **Container Scan settings**).

Container monitoring settings

Setting	Description
Namespace and container	This toggle switch enables or disables the scanning of namespaces and

scan enabled / disabled	containers in real time. The check toggle button is switched on by default.
Action with container upon threat detection	You can select the action that the application performs on a container when it detects an infected object: • **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.
Use Docker	This check box enables or disables the use of the Docker environment. The 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. The 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. The 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. The 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.

Configuring container monitoring in the Administration Console

In the Administration Console, you can manage the operation of the Container Monitoring component in the policy properties (Application settings → **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. The 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 environment. The 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. The 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. The 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.
Use runc	The check box enables or disables the use of the runc utility.

	The 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.

Configuring container monitoring in the command line

In the command line, you can enable or disable real-time scanning 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 keys.

When scanning namespaces and containers in real time, the general Container Scan settings are used. You can view and edit these settings using special administration commands for Kaspersky Endpoint Security:

- You can output the current values of general Container Scan settings to the console or to a configuration file. You can use this file to edit the settings.
- You can edit all general 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 edit individual settings using command line keys in the format `<setting name>=<setting value>`. You can get the current values of the settings using the command for displaying general Container Scan settings.

To output the current values of general Container Scan settings to the console, execute the following command:

```
kesl-control --get-container-settings [--json]
```

where `--json` is specified to output the settings in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

To output the current values of general Container Scan settings to a file, execute the following command:

```
kesl-control --get-container-settings --file <path to configuration file> [--json]
```

where:

- `--file <path to configuration file>` is the path to the file where the general Container 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` key is not specified, the settings will be imported in the INI format.

To edit the values of the general Container Scan settings using a configuration file:

1. Output the general Container 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. Execute the 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 the General Container Scan settings.
   - `--json`: specify this key if you are importing settings from a configuration file in JSON format. If the `--json` key 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 Container Scan settings defined in the file will be imported into the application.

To edit values of general Container Scan settings using command line keys, execute the following command:

`kesl-control --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]`

where `<setting name>=<setting value>` is the name and value of one of the general Container Scan settings.

The values of the specified general Container Scan settings will be changed.

On-demand scan of containers and images

When the *Container Scan* task is running, Kaspersky Endpoint Security scans containers and images for viruses and other malware. The application can run multiple Container Scan tasks simultaneously.

Integration with Docker container management system, CRI-O framework, and Podman and runc utilities is supported.

To use the task, a license that includes the corresponding function is required.

You can start a Container Scan and configure the settings of the scan:

- Specify the containers and images to be scanned by name or name mask.
- Enables scanning of all layers of images and containers.
- Select the action that the application will perform on the container and the action that the application will perform on the image when an infected object is detected.
- Configure settings for scanning objects inside containers or images:
  - Enable or disable scanning of archives, mail databases, email messages in text format.
  - Limit the size of an object to be scanned and the duration of the object scan.

- Select the actions to be performed by the application on the infected objects.
- Configure exclusions of objects from scans:
  - by name or mask
  - by the name of the threats detected in the objects
- Enable or disable the use of global exclusions when scanning.
- Configure the use of the heuristic analyzer and iChecker technology during a scan.
- Enable or disable the logging of information about scanned non-infected objects, about scanning objects in archives, and about unprocessed objects.

Container Scan in the Web Console

In the Web Console, you can scan containers and images using the *Container Scan* task.

You can create and run Container Scan user tasks. You can configure the scan settings by editing the settings of the tasks.

Container scan task 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. The 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 unchecked. The 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. Available 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. Available 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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.

First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Skip** the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Skip** the object (default value).
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. The 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	You can select the action that the application performs on a container when it detects an infected object: • **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 to select 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. The 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	You can select the action that the application performs on a container when it detects an infected object:

	• **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.

Exclusion scopes section

In the **Exclusion scopes** section for the Container Scan task, you can configure exclusions by mask and by threat name, as well as the use of global exclusions when the task is running.

Settings of scan exclusions

Setting	Description
Configure exclusions by mask	Clicking the **Configure exclusions by mask** link opens the **Exclusions by mask** window. In this window, you can configure the exclusion of objects from scans by name mask.
Configure exclusions by threat name	Clicking the **Configure exclusions by threat name** link 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. The check box is selected by default.

Exclusions by mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Container Scan in the Administration Console

In the Administration Console, you can scan containers and images using the *Container Scan* task.

You can create and run Container Scan user tasks. You can configure the scan settings by editing the settings of the tasks.

In the **Settings** section of the properties of the Container Scan task, you can configure 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.
Action on threat detection	This group of settings contains the **Configure** button. Clicking this button opens the **Action on threat detection** window, where you can configure the actions that the application performs on detected infected objects.

In the **Exclusions** section in the task properties, you can also configure exclusions by mask and by threat name for the Container Scan task.

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. The 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 to select 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. The 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.

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. The 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 unchecked. The 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. Available 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. Available 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	This check box enables or disables the logging *ObjectNotProcessed* type events if a file

unprocessed objects	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. The check box is selected by default.
Use heuristic analysis	This check box enables or disables heuristic analysis during file scans. The 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 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.

•

Action 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
First action	In this drop-down list, you can select the first action to be performed by the application on an infected object that has been detected: • **Disinfect** the object. A copy of the infected object will be moved to the Backup.

	• **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it (default value). • **Skip** the object.
Second action	In this drop-down list, you can select the second action to be performed by the application on an infected object, in case the first action is unsuccessful: • **Disinfect** the object. A copy of the infected object will be moved to the Backup. • **Remove** the object. A copy of the infected object will be moved to the Backup. • **Perform recommended action** on the object, based on data about the danger level of the threat detected in the file and about the possibility of disinfecting it. • **Skip** the object (default value).

•

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. The check box is selected by default.

Exclusions by mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected threat from the exclusion list.

This button is available if at least one threat name is selected in the list.

Clicking the threat name in the table opens the **Threat name** window. In this window, you can edit the name of the threat to be excluded from a scan.

Clicking the **Add** button opens the **Threat name** window. In this window, you can define the name of the threat to be excluded from a scan.

Container Scan in the command line

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 run 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 run schedule.
- Using the command `kesl-control --scan-container`, you can perform a *custom scan* of the specified containers and images.

Container scan task settings

The table describes all available values and the default values of all the container and image scan settings.

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 * characters.
	Before specifying this setting, make sure that `ScanContainers=Yes`.
		Default value: * (scan all containers).
		Examples:
		Scan a container with my_container name:
		`ContainerNameMask=my_container`
		Scan all containers whose names start with my_container:
		`ContainerNameMask=my_container*`
		Scan 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).
		Examples:
		Scan images with the "my_image" name, and the "latest" tag:
		`ImageNameMask=my_image:latest`
		Scan 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.

		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 to select 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.
`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 the `FirstAction=Recommended` value is specified, 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	0 – 9999

	(in seconds). The application stops scanning the object if it takes longer than the time specified by this setting.	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 – 999999 0 — The application scans objects of any size. Default value: 0.
`FirstAction`	Selection of the first action to be performed by the application on the infected objects.	`Disinfect` — The application tries to disinfect an object and save a copy of it to Backup. If disinfection fails (for example, if the type of object or the type of threat in the object cannot be disinfected), then the application leaves the object unchanged. If the first action is `Disinfect`, it is recommended to specify a second action using the `SecondAction` setting. `Remove` — The application removes the infected object after creating a backup copy of it. `Recommended` (perform recommended action) — The application automatically selects and performs an action on the object based on information about the threat detected in the object. For example Kaspersky Endpoint Security immediately removes Trojans since they do not incorporate themselves into other files and therefore they do not need to be disinfected. `Skip` — The application does not try to disinfect or delete infected objects. Information about the infected object is logged. Default value: `Recommended`.
`SecondAction`	Selection of the second action to be performed by the application on the infected objects. The application performs the second action if the first action fails.	The possible values of the `SecondAction` setting are the same as those of the `FirstAction` setting. If `Skip` or `Remove` is selected as the first action, the second action does not need to be specified. It is recommended to specify two actions in all other cases. If you have not specified the second action, the application applies `Skip` as the second action. Default value: `Skip`.
`UseExcludeMasks`	Uses scan exclusions for the objects specified by the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from scan `No` (default value) — Do not exclude objects specified by the `ExcludeMasks.item_#` setting from scans.
`ExcludeMasks.item_#`	Excludes objects from being scanned by name or mask. You	The default value is not defined.

	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.	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 scans. `No` (default value) — Do not exclude object containing the threats specified by the `ExcludeThreats.item_#` setting from scans.

`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 collect 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.	`Yes` — Log information about scanned objects within archives.

	You can enable this setting, for example, to make sure that an object within an archive has been scanned by the application.	`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.

Custom scan of containers and images

You can perform a custom scan of the specified containers and images using the 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).

To start the Custom Container Scan task, execute the following command:

```
kesl-control --scan-container <container/image [:tag ]>
```

where `<container/image [:tag ]>` is the name or ID of the container or image. You can use masks to scan multiple objects.

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.

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.

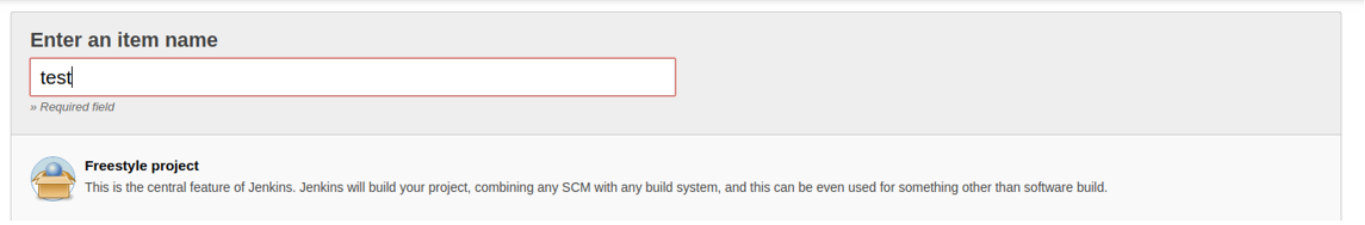
Examples:
Scan the container named my_container:
```
kesl-control --scan-container my_container
```
Scan the image named my_image (all tags):
```
kesl-control --scan-container my_image*
```

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:

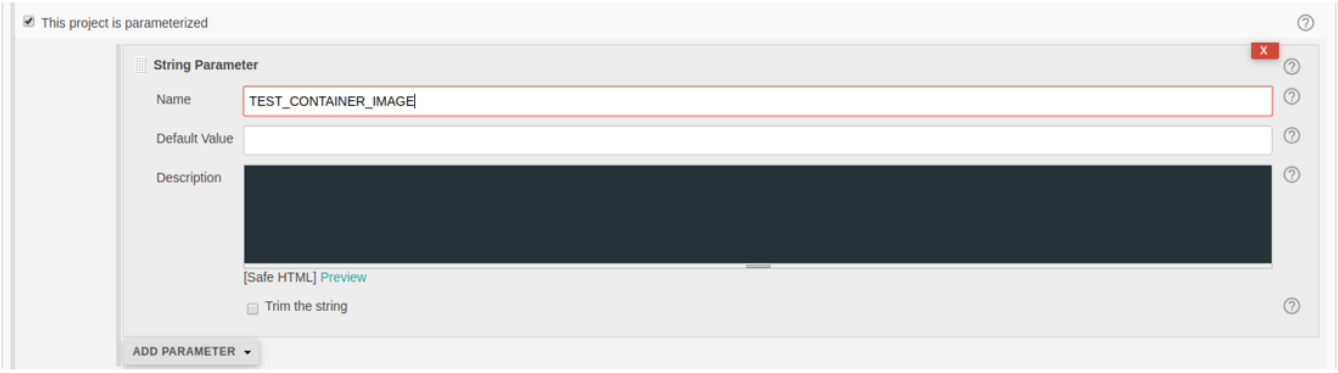
1. Install Kaspersky Endpoint Security on a Jenkins node.
2. Install Docker Engine on a Jenkins node.
   For details, please refer to the Docker Engine documentation.
3. Grant the Kaspersky Endpoint Security administrator privileges to the Jenkins user:
   ```
   kesl-control --grant-role admin <Jenkins 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.

Firewall Management

A device used on local area networks (LANs) and the internet is exposed to viruses, other malware, and a variety of attacks that exploit vulnerabilities in operating systems and software. The operating system firewall protects data stored on the user device by blocking most threats when the device is connected to the internet or a LAN.

The operating system's firewall can detect all network connections on the user's device and provide a list of their IP addresses. The Firewall Management component allows you to set the status of the network connections by configuring the network packet rules.

This feature is not supported in the KESL container.

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. All outbound connections are allowed by default, unless corresponding blocking rules for the Firewall Management component are specified.

The Firewall Management component is disabled by default.

It is recommended to disable other operating system firewall management tools before enabling the Firewall Management component.

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 required, save the custom firewall rules before enabling the Firewall Management component.

If firewall management is enabled, Kaspersky Endpoint Security scans the operating system firewall and blocks any attempt to change the firewall settings, for example, when an application or utility attempts to add or delete a firewall rule. Kaspersky Endpoint Security checks the operating system firewall every 60 seconds and, if necessary. restores the set of firewall rules created using the application. The checking period cannot be changed.

In the Red Hat Enterprise Linux and CentOS 8 operating systems, firewall rules created in Kaspersky Endpoint Security can only be viewed using administration commands (`kesl-control -F --query` command).

Kaspersky Endpoint Security still scans the operating system firewall when firewall management is disabled. This allows the application to restore dynamic rules.

You can enable or disable firewall management, and also configure the following settings:

- Configure a list of network packet rules that Kaspersky Endpoint Security will apply when an attempt to establish a network connection is detected. You can add or remove network packet rules, and also change the execution priority of a network packet rule.
- Select default actions to perform on incoming connections and packets if no other network packet rules apply to this connection type.
- Map network addresses to preset network zones. You can add IP addresses or subnets to network zones and delete address from network zones.
- Enables or disables automatic adding of allowing rules for Network Agent ports.

To avoid possible problems on systems with nftables, Kaspersky Endpoint Security uses the iptables and iptables-restore system utilities when adding rules for the firewall of the operating system. The application creates a special chain of allowing rules called kesl_bypass, and adds it at the top of the list in the mangle table of the iptables and ip6tables utilities. The rules of the kesl_bypass chain make it possible to exclude traffic from scans by Kaspersky Endpoint Security. The rules in this chain can be changed by means of the operating system. When the application is removed, the kesl_bypass rule chain is removed from iptables and ip6tables only if it was empty.

About network packet rules

Network packet rules are actions taken by the Kaspersky Endpoint Security to allow or deny a detected network connection attempt.

Network packet rules impose restrictions on network packets regardless of the application. Such rules restrict inbound and outbound network traffic through specific ports of the selected data protocol.

All outbound connections are allowed by default (default action setting), unless the corresponding blocking rules for the Firewall Management are specified. The default action is performed with the lowest priority: if no other network packet rule has been triggered or if no network packet rules have been specified, the connection is allowed.

Firewall Management specifies certain network packet rules by default. You can create your own network packet rules and specify an execution priority for each network packet rule.

About dynamic rules

Kaspersky Endpoint Security allows *dynamic rules* to be added to, or deleted from, the firewall to ensure the application works properly. For example, Network Agent adds dynamic rules that allow connections to Kaspersky Security Center initiated by the application or by Kaspersky Security Center. The rules of the Anti-Cryptor are also dynamic.

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 does not control dynamic rules and does not block application components' access to 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.

You can view the set of dynamic rules (using the `kesl-control -F --query` command); however the dynamic rules settings cannot be modified.

About the predefined network zone names

A *predefined network zone* is a specific group of IP addresses or subnets. Using a predefined network zone, you can use the same rules for several IP addresses or subnets without having to create a separate rule for each IP address or subnet. The network zone can be used as the value of the "remote address" parameter when creating a network packet rule. Kaspersky Endpoint Security has three predefined network zones with specific names:

- **Public**. Add a network address or subnet to this zone if it is assigned to networks that are not protected by any anti-virus applications, firewalls, or filters (for example, for Internet cafe networks).

- **Local**. Add a network address or subnet to this zone if it is assigned to networks whose users are trusted to access files and printers on this device (for example, a LAN or home network).
- **Trusted**. This zone is intended for a safe network in which the device is not exposed to attacks or unauthorized data access attempts.

You cannot create or delete a network zone. You can add or delete IP addresses and subnets to/from a network zone.

Firewall Management in the Web Console

In the Web Console, you can configure Firewall Management settings in the policy properties (**Application settings** → **Essential Threat Protection** → **Firewall Management**).

Firewall Management settings

Setting	Description
Firewall Management enabled / disabled	This toggle switch enables or disables Firewall Management. The toggle button is switched off by default.
Network packet rules	Clicking the **Configure network packet rules** link opens the **Network packet rules** window. In this window, you can configure the list of network packet rules that are applied by the Firewall Management component when it detects the network connection attempt.
Available networks	Clicking the **Configure available networks** link 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 automatic adding allowing rules for Network Agent ports. The 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.
Direction	Direction of the monitored network activity.
Protocol	Type of data transfer protocol for which network activity is monitored.
Local ports	Port numbers of local devices between which the connection is monitored.
Remote ports	Port numbers of remote devices between which the connection is monitored.
ICMP type	ICMP type. The Firewall Management component monitors messages of the specified type sent by a host or gateway.
ICMP code	ICMP code. The Firewall Management component monitors messages of the type specified in the **ICMP type** field and the code specified in the **ICMP code** field, sent by a host or gateway.
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.

Clicking the **Move down** button moves the selected item down in the table.

This button is available if only one item is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

This button is available if only one item is selected in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Network packet rule window

In this window, you can configure the network packet rule.

Network packet rule settings

Setting	Description
Rule name	The field for entering the name of the network packet rule.
Action	In the drop-down list, 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).
Protocol	In the drop-down list, 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**
Specify ICMP type	This check box lets you specify the ICMP type. The Firewall Management component monitors messages of the specified type sent by the host or gateway. If this check box is selected, the field for entering the ICMP type is displayed. This check box is displayed only if **ICMP** or **ICMPv6** data transfer protocol is selected in the **Protocol** drop-down list. This check box is cleared by default.
Specify ICMP code	This check box lets you specify the ICMP code. The Firewall Management component monitors messages of the type specified (in the field under the **Specify ICMP type** check box) and the code specified (in the field under the **Specify ICMP code** check box), sent by a host or gateway. If this check box is selected, the field for entering the ICMP code is displayed. This check box is displayed only if **ICMP** or **ICMPv6** data transfer protocol is selected in the **Protocol** drop-down list. It is available only if the **Specify ICMP type** check box is selected. This check box is cleared by default.
Direction	In this drop-down list, you can specify the direction of the monitored network activity: • **Incoming packets** (default value). If this option is selected, the Firewall Management component monitors incoming packets.

	• **Incoming**. If this option is selected, the Firewall Management component monitors incoming network activity. • **Incoming/Outgoing**. If this option is selected, the Firewall Management component monitors both incoming and outgoing network activity. • **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 outgoing packets. • **Outgoing**. If this option is selected, the Firewall Management component monitors outgoing network activity.
Remote address	In this drop-down list, you can specify network addresses of the remote devices that can send and receive network packets: • **Any address** (default value). If this option is selected, the network rule controls network packets sent and received by remote devices with any IP address. • **All subnet addresses**. If this option 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**. • **Specified address**. If this option is selected, the network rule controls network packets sent and received by the remote devices with IP addresses specified in the **Address** field.
Specify remote ports	This check box allows you to specify the port numbers of the remote devices between which the connection must be monitored. If this check box is selected, the field for entering port numbers is displayed. This check box is displayed only if **TCP** or **UDP** data transfer protocol is selected in the **Protocol** drop-down list. This check box is cleared by default.
Local address	In this drop-down list, 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 sending and receiving of network packets by the devices with Kaspersky Endpoint Security installed and with any IP address. • **Specified address**. If this option is selected, the network rule controls the specified in the **Address** field network addresses of the devices with Kaspersky Endpoint Security installed that can send and receive network packets.
Specify local ports	This check box allows you to specify the port numbers of the local devices between which the connection must be monitored. If this check box is selected, the field for entering port numbers is displayed. This check box is displayed only if **TCP** or **UDP** data transfer protocol is selected in the **Protocol** drop-down list. This check box is cleared by default.
Log events	This check box lets you specify whether the actions of the network rule are recorded in the report.

	If the check box is selected, the application writes the actions of the network rule to the report. If the check box is cleared, the application does not write the actions of the network rule to the report. This check box is cleared by default.

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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

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**

Firewall Management in the Administration Console

In the Administration Console, you can configure Firewall Management settings in the policy properties (Application settings → **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 automatic adding allowing rules for Network Agent ports. The 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	Network addresses of remote devices that can send and/or receive network packets.

address	
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.

Clicking the **Move down** button moves the selected item down in the table.

This button is available if only one item is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

This button is available if only one item is selected in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

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 incoming packets. • **Incoming**. If this option is selected, the Firewall Management component monitors incoming network activity. • **Incoming/Outgoing**. If this option is selected, the Firewall Management component monitors both incoming and outgoing network activity. • **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 outgoing packets. • **Outgoing**. If this option is selected, the Firewall Management component monitors outgoing network activity.
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 and the code specified in the **ICMP code** field, sent by a 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 the port numbers 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 the port numbers 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**. If this item 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 field below.

	• **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**. 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 field below.
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.

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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

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**

Firewall Management in the command line

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 a predefined task using the command for administering task settings.

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 Kaspersky Endpoint Security by using the command `kesl-control -F --query`.

Firewall Management task settings

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 inbound connections. `Outgoing` or `Out` — Monitor outbound connections. `IncomingPacket` or `InPacket` — Monitor incoming packets. `OutgoingPacket` or `OutPacket` — Monitor outgoing packets. `IncomingOutgoingPacket` or `InOutPacket` — Monitor both incoming and outgoing packets.
`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/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.
`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/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.
`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)
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 a list of network packet rules in the command line

To add a network packet rule, execute the following command:

```
kesl-control --add-rule [--name <rule name>] [--action <action>] [--protocol
<protocol>] [--direction <direction>] [--remote <remote address>[:<port range>]] [--
local <local address>[:<port range>]] [--at <index>]
```

where:

- `--name <rule name>` is the name of the network packet rule.
- `--action <action>` is the action to be performed on connections specified in network packet rule.
- `--protocol <protocol>` is the type of data transfer protocol for which you want to monitor network activity.
- `--direction <direction>` is the direction of the monitored network activity.
- `--remote <remote address>[:<port range>]>` 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 range>]>` is the network address of the device with Kaspersky Endpoint Security installed.
- `--at <index>` is the index of rules in the list of network packet rules. If the `--at` key 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.

Examples:
To create a rule that blocks all incoming and established connections to TCP port 23, execute the following command:
```
kesl-control --add-rule --name Block_Telnet --action Block --direction in --protocol
TCP --local any:23 --remote any
```
To create a rule that blocks incoming and established connections via the TCP port 23 for the Public network zone, execute the following command:
```
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>`
- `kesl-control --del-rule --index <index>`

where:

- `--name <rule name>` is the name of the network packet rule.
- `--index <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 <index>`
- `kesl-control --move-rule --index <index> --at <index>`

where:

- `--name <rule name>` is the name of the network packet rule.
- `--index <index>` is the current index of rules in the list of network packet rules.
- `--at <index>` is the new index of rules in the list of network packet rules.

Configuring network zones in the command line

To add a network address to the zone, execute the following command:

```
kesl-control --add-zone --zone <zone> --address <address>
```

where:

- `--zone <zone>` is the predefined name of the network zone. Possible values: `Public`, `Local`, `Trusted`.

- `--address <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 <zone> --address <address>`
- `kesl-control --del-zone --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.

Web Threat Protection

The Web Threat Protection component allows you to scan inbound traffic via HTTP, HTTPS, and FTP, websites, and IP addresses, prevent malicious files from being downloaded from the Internet, and block access to phishing, adware, and other malicious websites.

This feature is not supported in the KESL container.

Current connections for intercepted TCP ports are reset when Network Threat Protection is enabled.

By default, the Web Threat Protection task is disabled. However, it is enabled automatically if local management of Web Threat Protection settings has been allowed on the device (a policy is not applied or the "lock" is not set in the policy properties) and one of the following executable browser files, including in snap format, has been detected on the system:

- chrome
- chromium
- chromium-browser
- firefox
- firefox-esr
- google-chrome
- opera
- yandex-browser

You can enable or disable Web Threat Protection, and also configure the protection settings:

- Select action that the application performs on a web resource where a dangerous object is detected.
- Configure a list of trusted web addresses. The application will not scan the contents of websites whose web addresses are included in this list.
- Select objects that the application will detect when scanning inbound traffic.
- Configure the encrypted connections scan to scan HTTPS traffic.

  To scan FTP traffic, control of all network ports must be configured in the settings for the encrypted connections scan.

When a website is opened, the application performs the following actions:

1. Checks the website security using the downloaded application databases.
2. Checks the website security using heuristic analysis, if enabled.

During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of applications in the operating system. Heuristic analysis can detect dangerous objects for which there are currently no records in Kaspersky Endpoint Security databases.

3. Checks the trustworthiness of a website using Kaspersky reputation databases if the use of Kaspersky Security Network is enabled.

   You are advised to enable the use of Kaspersky Security Network to help Web Threat Protection work more effectively.

4. Blocks or allows opening of the website.

On attempt to open a dangerous website, the application performs the following:

- For HTTP or FTP traffic, the application blocks access and shows a warning message.
- For HTTPS traffic, a browser displays an error page.

Removing application certificates may cause the Web Threat Protection component to work incorrectly.

Kaspersky Endpoint Security adds a special chain of allowing rules (kesl_bypass) to the list in the mangle table of the iptables and ip6tables utilities. This chain of allowing rules makes it possible to exclude traffic from scans by the application. If traffic exclusion rules are configured in the chain, they affect the operation of the Web Threat Protection component.

Configuring Web Threat Protection in the Web Console

In the Web Console, you can configure Web Threat Protection settings in the policy properties (**Application settings** → **Essential Threat Protection** → **Web Threat Protection**).

Web Threat Protection component settings

Setting	Description
Web Threat Protection enabled / disabled	This toggle switch enables or disables the Web Threat Protection component. The toggle button is switched off by default.
Action on threat detection	In this section, you can specify the action that the application performs on the web resource where the dangerous object is detected: • **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. • **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).

Detect malicious objects	This check box enables or disables checking of links against the databases of malicious web addresses. The 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. The 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.
Trusted web addresses	This table contains addresses of URLs 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. 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). By default, the table is empty. You can add, edit, and remove web addresses in the table. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Web address window

In this window, you can add web addresses or web address masks to the list of trusted web addresses.

You can add only 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.

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).

Configuring Web Threat Protection in the Administration Console

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.

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).

You can add, edit, and remove web addresses on the list.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Web address window

In this window, you can add web addresses or web address masks to the list of trusted web addresses.

You can add only 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.

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. The 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. The 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.

Configuring Web Threat Protection in the command line

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.	`Inform` — 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`	Enables or disables checking of links against the databases 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`	Enables or disables checking of links against the databases 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`	Enables or disables the use of heuristic analysis for scanning web pages for phishing links.	`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.
`CheckAdware`	Enables or disables checking of links against the databases of adware 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`	Enables or disables the scanning of 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`	Enables or disables the usage of a 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_#` parameter.	`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. 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). Masks are not supported to specify IP addresses.

Encrypted connections scan

The settings for the encrypted connections scan are used in the operation of the Web Threat Protection and Web Control components. The Web Threat Protection component can decrypt and inspect network traffic sent over secure connections. The encrypted connections scan is enabled by default.

You can enable or disable the encrypted connections scan, and also configure the scan settings:

- Select the action to be performed by the application upon detection of an untrusted certificate.
- Select the action to be performed when an encrypted connections scan error occurs on a website.
- Enable or disable the use of the Internet for certificate verification.
- View and configure a list of trusted domains. The application will not scan encrypted connections established when visiting specified domains.
- Configure a list of certificates that the application will consider trusted when performing an encrypted connections scan.
- Configure a list of network ports to be monitored by the application. You can specify the network ports or network port ranges to be monitored.

When the encrypted connections scan settings are changed, the application records a *NetworkSettingsChanged* event in the log file.

Configuring encrypted connections scan in the Web Console

In the Web Console, you can configure settings for encrypted connections scans in the policy properties (**Application settings** → **General settings** → **Network settings**).

Encrypted connections scan settings

Setting	Description
Encrypted connections scan is enabled / disabled	This toggle switch enables or disables the encrypted connections scan. This toggle switch is turned on by default.
Trusted root certificates	Clicking **Manage trusted root certificates** opens the **Trusted root certificates** window, in which you can configure the list of trusted certificates. Trusted certificates are used when performing an encrypted connections scan.
Visiting a domain with an untrusted certificate	You can select the action that the application performs 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.
Visiting a domain with an encrypted	You can select the action that the application performs when a domain with an encrypted connections scan error is visited:

connections scan error	• **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	You can select how the application verifies certificates: • **Local check**: the application does not use the internet to validate a certificate. • **Full check** (default value): the application uses the Internet to check and download the missing chains that are required to validate a certificate.
Trusted domains	Clicking **Configure trusted domains** opens the **Trusted domains** window, in which you can configure the list of trusted domain names.
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 **Monitored ports** window. This option is selected by default.
Monitored ports	Clicking the **Configure network port settings** link opens the **Monitored ports** window, where you can specify the network ports to be monitored by the application.

Trusted certificates window

You can configure a list of certificates considered trusted by Kaspersky Endpoint Security. The list of trusted certificates is used when scanning encrypted connections.

The following information is displayed for each certificate:

- certificate subject
- serial number
- certificate issuer
- certificate start date
- certificate expiration date
- SHA256 certificate fingerprint

By default, the certificate list is empty.

You can add and remove certificates.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

Adding a trusted certificate window

In this window, you can add a certificate that will be trusted by Kaspersky Endpoint Security.

The **Add certificate** link opens the standard file selection window. Indicate the path to the file that contains the certificate, in DER or PEM format.

After the certificate file is selected, the window displays certificate information and the file path.

Trusted domains window

This list contains the domain names and domain name masks that will be excluded from encrypted connection scans.

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 and remove domains from the list of trusted domains.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Monitored ports

The table contains network ports that the application must monitor if in the **Network settings** window, under **Monitored port**, 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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Configuring encrypted connections scan in the Administration Console

In the Administration Console, you can configure settings for encrypted connections scans in the policy properties (**General settings** → **Network settings**).

Encrypted connections scan settings

Setting	Description
Enable encrypted connections scan	This check box enables or disables the encrypted connections scan. The check box is selected by default.
Visiting a domain with an untrusted certificate	In the drop-down list, you can select the action that the application performs 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.
Visiting a domain with an encrypted connections scan error	In the drop-down list, you can select the action that the application performs when a domain with an encrypted connections 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	In the drop-down list, you can select how the application verifies certificates: • **Local check**: the application does not use the internet to validate a certificate. • **Full check** (default value): the application uses the Internet to check and download the missing chains that are required to validate 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, which opens the Trusted root certificates window, where you can configure the list of trusted root certificates. Trusted certificates are used when performing an encrypted connections scan.
Network ports settings	This group of settings contains the **Configure** button. Clicking this button opens the Monitored ports window.

Trusted domains window

This list contains the domain names and domain name masks that will be excluded from encrypted connection scans.

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 and remove domains from the list of trusted domains.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Trusted certificates window

You can configure a list of certificates considered trusted by Kaspersky Endpoint Security. The list of trusted certificates is used when scanning encrypted connections.

The following information is displayed for each certificate:

- **Subject** – certificate subject
- **Serial number** – serial number of the certificate
- **Issuer** – issuer of the certificate
- **Valid from** – certificate start date
- **Expires on** – certificate expiration date
- **SHA256 fingerprint** is the SHA256 certificate fingerprint

By default, the certificate list is empty.

You can add and remove certificates.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

Adding certificate window

In this window, you can add a certificate to the trusted certificate list 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.

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 specified 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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Configuring encrypted connections scan in the command line

Special administration commands are provided in the command line for administering the settings for the encrypted connections scan. Using the commands for managing the settings for the encrypted connections scan, you can:

- Configure settings for the encrypted connections scan.
- View exclusions from the encrypted connections scan.
- Clear the list of domains that the application automatically excluded from the scan.
- Manage the list of certificates that the application considers to be trusted.

Viewing and editing settings for encrypted connections scan

You can view and edit the settings for the encrypted connections scan using special administration commands:

- You can output the current values of the settings for the encrypted connections scan to the console or to a configuration file. You can use this file to edit the settings.
- You can edit all the settings for the encrypted connections scan using the configuration file that contains the settings. You can get the configuration file using the command for displaying settings for the encrypted connections scan.
- You can edit individual settings using command line keys in the format `<setting name>=<setting value>`. You can get the current values of the settings using the command for displaying the settings for the encrypted connections scan.

To output the current values of the settings of the encrypted connections scan 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` key is not specified, the settings will be imported in the INI format.

To output the current values of the settings for the encrypted connections scan to a file, execute the following command:

```
kesl-control --get-net-settings --file <path to the configuration file> [--json]
```

where:

- `--file <path to the configuration file>` is a path to the configuration file where the settings for the encrypted connections scan 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` key is not specified, the settings will be imported in the INI format.

To edit the values of the settings for the encrypted connections scan using a configuration file:

1. Output the general application settings to a configuration file, as described above.
2. Edit the values of the necessary parameters in the file and save the changes.
3. Execute the command:

   `kesl-control --set-net-settings --file <path to configuration file> [--json]`

   where:

   - `--file <path to configuration file>` is the full path to the configuration file with the settings for the encrypted connections scan.
   - `--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` key 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 settings for the encrypted connections scan defined in the file will be imported into the application.

To edit the values of the settings for the encrypted connections scan using the command line, execute the following command:

`kesl-control --set-net-settings <setting name>=<setting value> [<setting name>=<setting value>]`

where `<setting name>=<setting value>` is the name and value of one of the settings for the encrypted connections scan.

The values of the specified settings for the encrypted connections scan will be changed.

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 secure connection scan exclusions added by a user, execute the following command:

```
kesl-control -N --query user
```

To view the list of secure connection scan exclusions added by a user, execute the following command:

```
kesl-control -N --query auto
```

To view the list of secured 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 a list of trusted certificates

To add a certificate to the trusted certificate list, run the following command:

```
kesl-control --add-certificate <path to certificate>
```

where:

`<path to certificate>` is the path to the certificate file that you want to add (PEM or DER format).

To remove a certificate from the trusted certificate list, run the following command:

```
kesl-control --remove-certificate <certificate subject>
```

To view the list of trusted 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

Network Threat Protection

The Network Threat Protection component allows you to scan inbound network traffic for activity that is typical for network attacks.

This feature is not supported in the KESL container.

Kaspersky Endpoint Security receives TCP port numbers from the current application databases and scans incoming traffic for these ports.

To scan network traffic, the Network Threat Protection task receives port numbers from the application databases and accepts connections via all these ports. During the network scan process, it may look like an open port on the device, even if no application on the system is listening to this port. It is recommended to close unused ports by means of a firewall.

Current connections for intercepted TCP ports are reset when Network Threat Protection is enabled.

If Network Threat Protection is enabled, upon detecting an attempted network attack on a protected device, the application blocks network activity from the attacking device and creates the *Network attack detected* event. The event contains information about the attacking device.

By default, network traffic from the attacking device is blocked for one hour. Once the blocking time has expired, the application unblocks the device.

Network Threat Protection is enabled by default if the Network Threat Protection settings on the device are defined through a policy. If locally configured settings are applied on the device, Network Threat Protection is disabled by default.

You can enable or disable Network Threat Protection, and also configure the protection settings:

- Select the action that the application will perform upon detection of network activity that is typical of network attacks.
- Enables or disables the blocking of network activity when a network attack attempt is detected.
- Set the duration for blocking an attacking device.
- Configure a list of IP addresses whose network activity will not be blocked by the application.

You can use the commands for administering blocked devices in the command line to view the list of blocked devices and manually unblock these devices. Kaspersky Security Center does not provide tools for monitoring and managing blocked devices, except for the *Network attack detected* events.

Kaspersky Endpoint Security adds a special chain of allowing rules (kesl_bypass) to the list in the mangle table of the iptables and ip6tables utilities. This chain of allowing rules makes it possible to exclude traffic from scans by the application. If traffic exclusion rules are configured in the chain, they affect the operation of the Network Threat Protection task. For example, to exclude outgoing HTTP traffic, you need to add the following command: `iptables -t mangle -I kesl_bypass -m tcp -p tcp --dport http -j ACCEPT`.

Configuring Network Threat Protection in the Web Console

In the Web Console, you can configure Network Threat Protection settings in the policy properties (**Application settings** → **Essential Threat Protection** → **Network Threat Protection**).

Network Threat Protection component settings

Setting	Description
Network Threat Protection enabled / disabled	This toggle switch enables or disables Network Threat Protection. The check toggle button is switched on 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).
Blocking attacking devices enabled / disabled	This toggle switch enables or disables blocking network activity when a network attack attempt is detected. The check toggle button is switched on 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. Available values: integer from 1 to 32768. Default value: 60.
Exclusions	The table contains a list of IP addresses. Network attacks from these addresses will not be blocked. By default, the list is empty. You can add, edit, and remove IP addresses in the table. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

IP address window

In this window, you can add and edit IP addresses. Network attacks from these IP addresses will not be blocked by Kaspersky Endpoint Security.

IP addresses

Setting	Description
Enter an IP address	Entry field for an IP address. You can specify IP addresses in IPv4 and IPv6 formats.

Configuring Network Threat Protection in the Administration Console

In the Administration Console, you can configure 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. The check box is selected 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. The 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. Available values: integer 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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

IP address window

In this window, you can add and edit IP addresses. Network attacks from these IP addresses will not be blocked by Kaspersky Endpoint Security.

IP addresses

Setting	Description
Enter an IP address	Entry field for an IP address. You can specify IP addresses in IPv4 and IPv6 formats.

Configuring Network Threat Protection in the command line

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`	Actions performed upon detection of network activity that is typical of network attacks. 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 – 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.

Protection against remote malicious encryption

Anti-Cryptor component allows you to protect your files in local directories with network access by SMB/NFS protocols from remote malicious encryption.

To use the component, a license that includes the corresponding function is required.

This feature is not supported in the KESL container.

If Anti-Cryptor is enabled, Kaspersky Endpoint Security scans the actions of remote devices with file resources located in shared network directories of the protected device for the presence of malicious encryption. If an application considers the actions of a remote device accessing shared network resources to be malicious encryption, the application creates and enables a rule for the firewall of the operating system that blocks network traffic from the compromised device. The compromised device is added to the list of untrusted devices, and access to shared network directories is blocked for all untrusted devices. The application creates an *Encryption detected* event that contains information about the compromised device.

By default, the application blocks access of untrusted devices to network file resources for 30 minutes. When the blocking time expires, the application deletes the compromised device from the list of untrusted devices, and the device's access to network file resources is automatically restored.

Firewall rules created by the Anti-Cryptor component cannot be deleted using the iptables utility, since the application restores a set of rules every minute.

Protection against remote malicious encryption is disabled by default.

You can enable or disable protection against malicious encryption (Anti-Cryptor), and also configure the protection settings:

- Select the action that the application will perform when encryption is detected: notify the user or block the device performing the malicious encryption.

  If the *Inform* action is selected, the application still scans remote devices' actions on network file shares to check for malicious encryption when Anti-Cryptor is enabled. If malicious activity is detected, the *Encryption detected* event is created, but the compromised device is not blocked.

- Set the duration for blocking an untrusted device.

- Specify the files and directories that the application protects against malicious encryption.

- Specify the files and directories that are excluded from protection against malicious encryption.

  The application does not consider actions to be encryption if encryption activity is detected in directories excluded from protection against encryption (Anti-Cryptor).

You can use the commands for administering blocked devices in the command line to view the list of blocked devices and manually unblock these devices. Kaspersky Security Center does not provide tools for monitoring and managing blocked devices, except for the *Encryption detected* events.

For the Anti-Cryptor component to operate correctly, at least one of the services (Samba or NFS) must be installed in the operating system. The NFS service requires the rpcbind package to be installed.

The Anti-Cryptor component runs correctly with SMB1, SMB2, SMB3, NFS3, TCP/UDP, and IP/IPv6 protocols. Working with NFS2 and NFS4 protocols is not supported. It is recommended to configure your server settings so that the NFS2 and NFS4 protocols cannot be used to mount resources.

Kaspersky Endpoint Security does not block access to network file resources until the device's activity is identified as malicious. So, at least one file will be encrypted before the application detects malicious activity.

Configuring Anti-Cryptor in the Web Console

In the Web Console, you can configure Anti-Cryptor settings in the policy properties (**Application settings** → **Advanced Threat Protection** → **Anti-Cryptor**).

Anti-Cryptor component settings

Setting	Description
Anti-Cryptor protection enabled / disabled	This toggle switch enables or disables the protection of files in the local directories with network access by SMB/NFS protocols from remote malicious encrypting. The toggle button is switched off by default.
Protection scopes	Clicking the **Configure protection scope** link opens the **Protection scopes** window.
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 device blocking duration in minutes. 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. Available values: integer from 1 to 4294967295. Default value: 30.
Exclusions	Clicking the **Configure exclusions** link opens the **Exclusion scopes** window.
Exclusions by mask	Clicking the **Configure exclusions by mask** link opens the **Exclusions by mask** window.

Protection scopes window

The table contains protection scopes of the Anti-Cryptor component. 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.

Protection scope settings

Setting	Description
Scope name	Protection 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.

Clicking the **Move down** button moves the selected item down in the table.

This button is available if only one item is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

This button is available if only one item is selected in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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 protects 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.

Add protection 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 **Protection 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. The check box is selected by default.
File system,	You can select the type of file system in the drop-down list:

access protocol, and path	• **Local** (default value) – local directories. • **Shared** displays server file system resources accessible via the Samba or NFS protocol. • **All shared** displays all server file system resources accessible via the Samba and NFS protocols.
Access protocol	You can select the remote access protocol in the drop-down list: • **NFS**: remote directories mounted on a device using the NFS protocol. • **Samba**: remote directories mounted on a device using the Samba protocol. This drop-down list is available if the **Shared** option is selected in the drop-down list of file systems.
Path	The entry field for specifying the path to the directory that you want to include in the protection scope. You can use masks to specify the path. 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. This field is available if the **Local** type is selected in the drop-down list of file systems. The field must not be blank. By default, the **/** path is specified (root directory).
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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Exclusion scopes window

This table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

Add exclusion scope window

In this window, you can add and configure 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	This check box enables or disables the exclusion of the scope when the application is running. If the check box is selected, the application excludes this scope from scan or protection during its operation. If the check box is cleared, the application includes this scope in scan or protection during its operation. You can later exclude this scope from scan or protection by selecting the check box. The check box is selected by default.
File system, access protocol, and path	In this drop-down list, you can select the type of file system where the directories that you want to add to scan exclusions are located: • **Local**, for local directories.

	• **Mounted**, for remote directories mounted on the device. • **All remote mounted** – all remote directories mounted on the device using the Samba and NFS protocols.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Mounted** type is selected in the drop-down list of file systems.
Path	Entry field for the path to the directory that you want to add to the exclusion scope. You can use masks and tags to specify the path. You can use special tags to specify a container or image: • `[container-id:<identifier>]/<path to local directory>` • `[container-name:<name>]/<path to local directory>` • `[image-id:<identifier>]/<path to local directory>` • `[image-name:<name>]/<path to local directory>` You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags. 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:<identifier>][image-name:<name>]/<path to local directory>` • `[image-name:<name>][image-id:<identifier>]/<path to local directory>` • `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>` • `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>` You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. The **/** path is specified by default. The application excludes all directories of the local file system from scan. This field is available if the **Local** type is selected in the drop-down list of file systems.
Name of shared resource	The field for entering the name of the file system shared resource, 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 File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.
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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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).

Configuring Anti-Cryptor in the Administration Console

In the Administration Console, you can configure Anti-Cryptor settings in the policy properties (**Advanced Threat Protection → Anti-Cryptor**).

Anti-Cryptor component settings

Setting	Description
Enable	This check box enables or disables the protection of files in local directories with network

Anti-Cryptor	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. The 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.

	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. To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk). The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself. You can use a single ? character to represent any one character in the file or directory name. 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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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 device 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. Available values: integer from 1 to 4294967295. Default value: 30.

Exclusion scopes window

This table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

<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	The check box enables or disables exclusion of the scope from scan when the application is

scope	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. The 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.

You can use special tags to specify a container or image:

- `[container-id:<identifier>]/<path to local directory>`
- `[container-name:<name>]/<path to local directory>`
- `[image-id:<identifier>]/<path to local directory>`
- `[image-name:<name>]/<path to local directory>`

You can also use unique combinations of the `[container-id:<identifier>]`, `[container-name:<name>]`, `[image-id:<identifier>]` and `[image-name:<name>]/<path to local directory>` tags.

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:<identifier>][image-name:<name>]/<path to local directory>`
- `[image-name:<name>][image-id:<identifier>]/<path to local directory>`
- `[container-name:<name>][container-id:<identifier>][image-name:<name>]/<path to local directory>`
- `[container-name:<name>][image-id:<identifier>][container-id:<identifier>][image-name:<name>]/<path to local directory>`

You can use masks (`?` and `*` characters) in names and identifiers.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. 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. Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan. This button is available if at least one file mask is selected in the list. Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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 mask window

You can configure the exclusion of objects from scans based on 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 **Delete** button causes Kaspersky Endpoint Security to remove the selected name mask of files excluded from a scan.

This button is available if at least one file mask is selected in the list.

Clicking the mask opens the **Object mask** window. In this window, in the **Define object mask** field, you can modify the name template for files that Kaspersky Endpoint Security excludes from scans.

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).

Configuring Anti-Cryptor in the command line

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 protection scope exclusions for objects specified by the `ExcludeMasks.item_#` setting. This setting only applies if a value is specified for the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from the protection scope. `No` (default value) — Do not exclude 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`.
`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.	Default value: * (protect all objects)

	You can specify several `AreaMask.item_#` items in any order. The application processes the scopes by index in ascending order.	
`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. 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. `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. 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.

		`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.

Managing 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:

- If malicious encryption is detected, the application blocks access of the remote device to the shared network directories of the protected device.
- Upon detecting network attack attempts on the protected device, the application blocks network traffic from the attacking device.

You can change the blocking duration in the Network Threat Protection and Protection Against Remote Malicious Encryption settings. Once the specified period of time has elapsed, the application unblocks the device.

If you are managing the application using the command line, you can use the commands for managing blocked devices to view a list of devices that are blocked as a result of the application running on the device and manually unblock these devices before the blocking time expires. Kaspersky Security Center does not provide tools for monitoring and managing blocked devices, except for the *Network attack detected* and *Encryption detected* events.

-H is a prefix indicating that the command belongs to the group of commands for managing devices blocked by Anti-Cryptor and Network Threat Protection.

The kesl-control --get-blocked-hosts command

The command allows you to output the list of blocked devices to the console.

Command syntax

```
kesl-control [-H] --get-blocked-hosts
```

The kesl-control --allow-hosts command

The command allows you to unblock blocked devices.

Command syntax

```
kesl-control [-H] --allow-hosts <address>
```

Arguments and keys

`<address>` is an IP address of the 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.

To view the list of blocked devices, execute the following command:

```
kesl-control --get-blocked-hosts
```

As a result of the command execution, the application outputs the list of blocked devices to the console.

To unblock devices, execute the following command:

```
kesl-control --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.

As a result of the command execution, the application unblocks the specified devices.

Examples:
IPv4 addresses:

```
dec - 192.168.0.1
dec - 192.168.0.0/24
```

IPv6 addresses:

```
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
hex - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210%1
hex - 2001:db8::ae21:ad12
hex - ::ffff:255.255.255.254
hex - ::
```

Application Control

The Application Control component allows you to manage the launch of applications on protected devices. Application Control lowers the risk of device infection by limiting users' access to applications.

To use the component, a license that includes the corresponding function is required.

This feature is not supported in the KESL container.

Application launching is regulated by *Application Control rules*.

The Application Control component can operate in one of two modes:

- *Denylist*. In this mode Kaspersky Endpoint Security allows all users to launch any applications that are not specified in the Application Control rules. By default, the Application Control component operates in this mode.
- *Allowlist*. In this mode Kaspersky Endpoint Security prevents all users from launching any applications that are not specified in the Application Control rules.

If the Application Control rules are created to the fullest extent possible, Kaspersky Endpoint Security prohibits the launching of all new applications that are not verified by the administrator of the organization's local network, but ensures the performance of the operating system and verified applications that users need to perform their job duties.

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.

Application Control is disabled by default. You can enable or disable Application Control, and also configure the component's operation settings:

- Select the Application Control mode: *allowlist* or *denylist*.
- Create Application Control rules for each of the modes.
- Select the action that Kaspersky Endpoint Security will perform upon detecting an attempt to start an application that matches the rules: *apply the rules* or *test rules* and notify about an attempt to start an application that matches the rules.

You can receive information about applications installed on protected devices using the Inventory task.

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 interpreter is allowed to launch by the Application Control rules, Kaspersky Endpoint Security does not block the script launched from this interpreter. If the launch of at least one script specified in the interpreter command line is prohibited by the Application Control rules, Kaspersky Endpoint Security blocks all the scripts specified in the interpreter command line. Exclusion: cat script.py | python.

About Application Control rules

An *Application Control rule* is a set of settings that contain the conditions for triggering a rule and the actions of the Application Control component when a rule is triggered (allowing or blocking users when starting the application):

- The application belonging to the application category. An *application category* is a group of applications with common characteristics. For example, a category that includes executable files of installed applications, or a category of applications required for operation, which includes a standard set of applications used by the organization. Each category can only be used in one rule.

  Kaspersky Endpoint Security does not support use of the KL categories of Kaspersky Security Center.

- Permission or prohibition for selected users and/or user groups to run applications. You can specify a user and/or user group that is allowed or not allowed to run applications of the specified category.

- Rule triggering condition. A condition is represented by the following correspondence: "condition type – condition criterion – condition value". Based on the rule triggering condition, Kaspersky Endpoint Security applies or does not apply the rule to the application. The rules use inclusive and exclusive conditions:

  - *Inclusive conditions*. Kaspersky Endpoint Security applies the rule to the application if the application meets at least one inclusive condition.

  - *Exclusive conditions*. Kaspersky Endpoint Security does 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.

  Rule triggering conditions are created using the following criteria:

  - 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 is allowed.

  For each criterion used in the condition, a value must be specified.

  You can use masks to specify the names of files and directories.

  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.

  If the settings of the application being launched match the criteria specified in the inclusive condition, the rule is triggered. In this case, Kaspersky Endpoint Security performs the action specified in the rule. If application settings match the criteria specified in the exclusive condition, Kaspersky Endpoint Security does not control the application launch.

Application control rules can have one of the following *operation statuses*:

- *Enabled*: the rule is enabled, Kaspersky Endpoint Security applies this rule for the Application Control.
- *Disabled*: the rule is disabled and is not used for the Application Control.
- *Test* – Kaspersky Endpoint Security allows launching applications that meet the rule criteria, but logs information about launches of these applications in the report.

The priority of the rule operation status is higher than the priority of the action specified in the rule.

Configuring Application Control in the Web Console

In the Web Console, you can configure Application Control settings in the policy properties (**Application settings** → **Security Controls**→ **Application Control**)

Application Control component settings

Setting	Description
Application Control enabled / disabled	This toggle switch enables or disables Application Control. The toggle switch is off by default.
Action on starting applications blocked by rules	The action that Kaspersky Endpoint Security performs upon detecting an attempt to start an application that matches the configured 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. • **Apply rules** (default value). If you select this option, Kaspersky Endpoint Security applies Application Control rules and performs the action specified in 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	Clicking the **Configure rules** link 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). When you select this item, the application applies the rules specified in the policy together with the local rules configured on the protected device.

Application Control rules window

The **Application Control rules** table has the tabs with the rules for each operation mode: **Denylist (active)** and **Allowlist**. Both tabs of the Application Control rules table are empty by default.

Application Control rules settings

Setting	Description
Category	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 add, modify and remove Application Control rules.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

Application Control rule window

In this window, you can configure the settings for the Application Control rule.

Configuring an Application Control rule

Setting	Description
Rule description	Description of the Application Control rule.
Status	You can select the 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.
Category	The **Choose category** link 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** – access type (allow or block launching applications). This toggle switch switches access type: **Allow** launching the applications or **Block** launching the applications.

  You can add, edit, and delete users or user groups.

  Clicking the **Delete** button removes the selected item from the table.

  This button is available if at least one item is selected in the table.

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	Search bar for added application categories.
Add	Clicking the button starts the category creation wizard. Follow the instructions of the Wizard.
Edit	Clicking this button opens the category properties window, where you can change the category settings.
Remove	Clicking the button deletes the selected category. The **Golden Image (local)** category cannot be deleted.

Select 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.

Configuring an Application Control rule

Setting	Description
Manual	If this option is selected, in the field below enter the name of the local or domain user or the name of a user group, to which the Application Control rule will apply.
List of groups or users	If this option is selected, in the search field you can enter search criteria for the name of the user or name of the user group, to which the Application Control rule will apply, or you can select the name of the user group in the list below.

Configuring Application Control in the Administration Console

In the Administration Console, you can configure 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). When you select this item, the application applies the rules specified in the policy together with the 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 / Edit rule** window.

You can add, modify and remove Application Control rules.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

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, and delete users or user groups. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table.

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.
Edit	Clicking this button opens the category properties window, where you can change the category settings.

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.

Configuring Application Control in the command line

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 the command line keys, run the `kesl-control --set-settings` command with the `--accept` flag.

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 settings

The table describes all available values and the default values of all the settings that you can specify for the Application Control task.

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.

		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.
`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. 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.
`IncludeHashes.item_#`	SHA256 hash of the executable file that triggers the rule.	Only SHA256 is allowed.
`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.

		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.
`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. 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.
`ExcludeHashes.item_#`	SHA256 hash of the executable file that triggers the rule.	Only SHA256 is allowed.
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>`: name of the user to whom the rule applies. `@<group name>`: name of the group of users to whom 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	`\Everyone` (default value): the rule

	applies.	applies to all users. < user name >: name of the user to whom the rule applies. @< group name >: name of the group of users to whom the rule applies.

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 configuration file>
```

where:

`--file <path to configuration file>` – path to the configuration file with the category settings.

The file with category settings must have the following structure:

```
[
   {
     "Exclude": ["(FilePath like <full path to the executable file>)", "(FileHash ==
    <executable file hash>)"],
     "GUID" : "<unique category ID>",
     "Include" : [ "(FilePath like <full path to executable file>)", "(FileHash ==
    <executable file hash>)" ],
     "Name" : "<name of category 1>"
   },
   {
     "Exclude": ["(FilePath like <full path to the executable file>)", "(FileHash ==
    <executable file hash>)"],
     "GUID" : "<unique category ID>",
     "Include" : [ "(FilePath like <full path to executable file>)", "(FileHash ==
    <executable file hash>)" ],
     "Name" : "<name of category 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 is displayed and the category is not created. The `GUID` setting must be specified without hyphens.

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.

To edit the list of created application categories, run the following command:

```
kesl-control --set-categories [--names <name of category 1> <name of category 2> ...
<name of category N>] --file <path to configuration file>
```

where:

- `<name of category 1> <name of category 2> ... <name of category N>` – names of the categories whose information you want to change. 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 configuration file>` – path to the configuration file with the category settings.

Viewing the list of created categories

In the command line, you can view the list of created application categories using the Application Control administration command.

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 configuration file>] [--json]
```

where:

- `--file <path to configuration file>` – full path to the JSON configuration file to which the settings will be output.
- `--json` is specified to output the settings in JSON format. If the --json key is omitted, the settings are output in the INI 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 created application categories, execute the following command:

```
kesl-control --get-categories [--names <name of category 1> <name of category 2> ...
<name of category N>] [--file <path to configuration file>] [--json]
```

where:

- `<name of category 1> <name of category 2> ... <name of category N>` – names of the categories whose information you want to view. If you want to view information about several categories, specify the names of the categories, separated by a space.
- `--file <path to 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 the --json key is omitted, the settings are output in the INI format.

If in the Application Control task settings in the `[Categories.item_#]` section for including or excluding 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 refers will be 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 configuration file>] [--json]
```

where:

`--file <path to configuration file>` – full path to the configuration file to which the settings will be exported.

`--json`: output data in JSON format.

Kaspersky Endpoint Security displays the following information about Application Control rules:

- Application Control task operation mode;
- the 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;
- User 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 configuration file>] [--json]
```

where:

`--file <path to configuration file>` – full path to the configuration file from which the settings will be imported.

`--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
```

Inventory

The Inventory task provides information about all applications executable files stored on the client devices. Obtaining information about the applications installed on the devices can be useful, for example, for creating Application Control rules.

This feature is not supported in the KESL container.

To use the task, a license that includes the corresponding function is required.

You can configure the following inventory settings:

- Select the types of objects that the application will detect on the device during inventory (files, scripts).
- Enables or disables adding applications detected on the device by the Inventory task to the "Golden Image" category.
- Configure inventory scopes (paths to directories in which to search for executable application files).
- Configure exclusions from the inventory.

Inventory in the Web Console

In the Web 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 configure inventory settings by editing the settings of these 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
Add files to the Golden Image category	The check box enables or disables adding applications detected on the device by the Inventory task to the Golden Image category. If the check box is selected, you can use the "Golden Image" category in the Application Control rules. This check box is cleared by default.
Scan all executables	This check box enables or disables of executable file scans. The check box is selected by default.
Scan binaries	This check box enables or disables of binary file scans (with extensions elf, java, and pyc). The check box is selected by default.
Scan	This check box enables or disables script scans.

scripts	The check box is selected by default.
Inventory scopes	The table contains the inventory scopes scanned by the application. The application will scan files and directories located in the paths specified in the table. By default, the table contains one inventory scope – /usr/bin. You can add, configure, delete, move up, or move down inventory scopes 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. Clicking the scan scope name opens the **<Scan scope name>** window. In this window, you can modify the settings of the selected scan scope. Clicking the **Add** button opens the **<New scan scope>** window. In this window, you can define a new scan scope.

Add scan scope window

In this window, you can add and configure scan scope for the Inventory task.

Inventory scope settings

Setting	Description
Scope name	Field for entering the inventory scope name. This name will be displayed in the table in the **Scan settings** section. 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 inventory scope while running the task. If this check box is cleared, the application does not process this inventory scope while running the task. You can later include this scope in task settings by selecting the check box. The 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 inventory scope. You can use masks to specify the path. 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. The field must not be blank. The **/** path is specified by default – the application scans all directories of the local file system.
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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Exclusion scopes section

In the **Exclusion scopes** section for the Inventory task, you can configure the scopes to be excluded from scans.

Exclusion scopes window

This table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

Add 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. The 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.

	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. 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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Inventory in the Administration Console

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 configure the 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
Add files to the Golden	The check box enables or disables adding applications detected on the device by the Inventory task to the Golden Image category. If the check box is selected, you can use the

Image category	"Golden Image" category in the Application Control rules. This check box is cleared by default.
Scan all executables	This check box enables or disables of executable file scans. The check box is selected by default.
Scan binaries	This check box enables or disables of binary file scans (with extensions elf, java, and pyc). The check box is selected by default.
Scan scripts	This check box enables or disables script scans. The 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 **Exclusion scopes** 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.

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 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. The 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. 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. 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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

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 table contains scan exclusion scopes. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

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.

You can add, edit, and delete items 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.

<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. The 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. 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.
Masks	The list contains name masks of the objects that the application excludes from scan. You can add, edit, or delete masks. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table. The selected element's settings are changed in a separate window.

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).

Inventory in the command line

You can use the command line to inventory applications on the protected device as follows:

- With the help of the Inventory_Scan *predefined task*. You can manually start or stop this task, and configure the task run schedule. You can configure scan settings by editing the settings of this task.
- With the help of user inventory tasks (*InventoryScan*-type tasks). 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 settings

The table describes all available values and the default values of all the settings that you can specify for the Inventory task.

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.
`CreateGoldenImage`	Adds applications detected on the device by the Inventory task to the Golden Image category. If `CreateGoldenImage=Yes`, then you can	`Yes` – add detected applications to the "Golden Image" application category.

	use the "Golden Image" application category in the Application Control rules.	`No` (default value) – do not add detected applications to the "Golden Image" application category.
The **[ScanScope.item_#]** section contains the following settings:		
`AreaDesc`	Description of inventory scope; contains additional information about 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 scope limitation. In the inventory 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; contains additional information about the inventory 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 >` — Exclude objects in the specified directory from scan. You can use masks to specify the path.

		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 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.

Device Control

The *Device Control* component allows you to manage user access to the devices that are installed on or connected to the client device (for example, hard drives, cameras, or Wi-Fi modules). Access management lets you protect the client device from infection when external devices are connected, and prevent data loss or leaks.

This feature is not supported in the KESL container.

The Device Control component is enabled automatically with the default settings when Kaspersky Endpoint Security starts.

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*, to 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.
  - *By rule*: allow or block access to devices depending on the 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.

    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 will be blocked.
- **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.

By default, the *Depends on connection 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.

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. 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.

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.

When Device Control is disabled, the application unblocks access to blocked devices.

You can enable, disable, and configure Device Control:

- Select the application's operation mode when there is an attempt to access a device to which access is prohibited by Device Control settings: block or only notify about the attempt to access the device.
- Select a device access mode depending on the type.
- Select an access mode for the bus through which the devices are connecting.
- Remove individual devices from the scope of Device Control by adding them to the list of trusted devices. *Trusted devices* are devices to which users have full access. You can add devices to a list of trusted devices by identifier or identifier mask. For example, you can limit access to specific USB devices or only to USB drives; access to other USB devices is denied.

  If you are managing the application via the command line, you can view the IDs of connected devices by running `kesl-control --get-device-list` on the client device.

  If you are managing the application via Kaspersky Security Center, information about devices installed on, or connected to, the client devices can be sent to the Administration Server. The information sharing is enabled by default.

  > Information about devices is transferred if the client device is under the control of an active policy and synchronized with Network Agent (performed with the frequency specified in the Network Agent policy properties, by default – every 15 minutes).

- Define an access schedule for devices: only hard drives, removable drives, floppy disks, and CD/DVD drives.

  > 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.

- You can define access rules for devices depending on their type. Allow or block access for specified users at a specified time.

Device Control ignores mount point exclusions. Access to a device mounted at an excluded point can be limited with Device Control settings.

Configuring Device Control in the Web Console

In the Web Console, you can configure Device Control settings in the policy properties (**Application settings** → **Security Controls**→ **Device Control**)

Device Control settings

Setting	Description
Device Control enabled / disabled	This toggle switch enables or disables Device Control. The check toggle button is switched on by default.
Configure trusted devices	Clicking this link opens the **Trusted devices** window. In this window, you can add devices to a list of trusted devices by ID or by selecting them from the list of devices detected on the client devices.
Device Control	Response to attempts to access a device that is restricted according to Device

operating mode	Control rules: • **Inform**. If you select this option, Kaspersky Endpoint Security tests the selected access mode and generates an event about detection of an attempt to access a device. • **Block** (default value). When this option is selected, Kaspersky Endpoint Security applies the access mode defined for the device or bus.
Configure access settings for device types	Clicking this link opens the **Device types** window. In this window, you can configure access to devices by type.
Configure access settings for connection buses	Clicking this link opens the **Connection buses** window. In this window, you can configure access settings for connection buses.

Trusted devices window

The table contains a list of trusted devices. The table is empty by default.

Trusted device settings

Setting	Description
Device ID	Trusted device ID.
Device name	Trusted device name.
Device type	Trusted device type (for example, Hard drive or Smart card reader).
Host name	Host name the trusted device is connected to.
Comment	Comment related to a trusted device.

You can add a device to the list of trusted devices by the device ID or by selecting the required device in the list of devices detected on the user device.

You can edit and delete trusted devices in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

You can also import the list of devices from a file by clicking **Import** and export the list of added devices to a file by clicking **Export**. When importing, you will be prompted to replace the list of trusted devices or add the devices to the existing list.

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	Entry field for a device ID or device ID mask. You can manually specify the device ID or copy the ID of the required device from the **Devices detected on hosts** list. 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.
Comment	Entry field for a comment (optional). This field is available after you enter the device ID, and click the **Next** button.

Trusted device window (List of detected 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 there is an active policy and there has been synchronization with the Network Agent (performed with the frequency specified in the Network Agent policy properties, 15 minutes by default). If you create a new policy and there are no other active ones, the list will be empty.

Adding device from list

Setting	Description
Device type	In this drop-down list, you can select type of devices to be displayed in the **Devices detected on hosts** table.
Device ID mask	Entry field for a device ID mask.
Comment	Entry field for a comment (optional). This field is available after you select the devices, and click the **Next** button.

Clicking the **Filter** button opens the window, where you can set up the filtering of displayed information about devices.

Device types window

In this window, you can configure access rules for various types of devices.

Access rules for device types

Setting	Description

Settings for access to data storage devices	The table contains the following columns:
	• **Type** represents device types (for example, Hard drives, Printers).
	• **Access mode** represents the access mode for this type of device. You can choose one of the following access modes:
	  • **Allow**, to allow access to devices of this type.
	  • **Block**, to block access to devices of this type.
	  • **Depends on bus** (default value), to allow or block access to devices depending on the access mode for a bus used for connecting a device.

	• **By rule** – allow or block access to devices, depending on the access rule and schedule. You can configure the access rule and its schedule by clicking the required device type.

Settings for access to other devices	The table contains the following columns:
	• **Type** – type of device (for example, Input devices, Sound adapters).
	• **Access mode** represents the access mode for this type of device. You can choose one of the following access modes:
	  • **Allow**, to allow access to devices of this type.
	  • **Block**, to block access to devices of this type. The **Block** access mode cannot be selected for network adapters.
	  • **Depends on bus** (default value), to allow or block access to devices depending on the access mode for a bus used for connecting a device.

Device access settings window

In this window, you can configure the access mode and access rules for the selected type of device.

Device access settings

Setting	Description
Device access mode	Access mode for devices of the selected type: • **Allow**: allow access to devices of the selected type. • **Block**: prohibit access to devices of the selected type. • **Depends on bus** (default value), to allow or block access to devices depending on the access rule for a bus used for connecting a device. • **By rule** – allow or block access to devices, depending on the access rule and schedule.

Device access rules	The table contains a list of access rules and consists of the following columns:
	• **Access schedule** – names of existing access schedules.
	• **Users and/or user groups** – names of users or names of user groups, to which the access rule will apply.
	• **Access** – access mode for the schedule:
	  • **Allow** (provides access to devices of the selected type).
	  • **Block** (prohibits access to devices of the selected type).
	• **Status** – status of the access rule:
	  • **Enabled** – the rule is enabled; Application Control applies this rule when it runs.
	  • **Disabled** – the rule is disabled and is not used when Application Control is running.

	By default, the table contains the **Default schedule** access schedule, which provides all users with full access to devices (the **\Everyone** option is selected in the list of users and groups) at any time, if access by the connection bus is allowed for this type of device. You can add, edit, and delete access rules. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table.

Device access rules window

In this window, you can configure the device access rule.

Device access rule

Setting	Description
Device access rule settings	Access mode for devices of the selected type: • **Allow** (default value) – provide access to the devices of the selected type. • **Block**: prohibit access to devices of the selected type.
Users and/or user groups	Name of the user or user group to which the rule applies. The default value is **\All** (all users). You can add, edit, and delete users or user groups. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table.
Status	Access rule status: • **Enabled** – the rule is enabled; Application Control applies this rule when it runs. • **Disabled** – the rule is disabled and is not used when Application Control is running.
Schedule for access to devices	Schedule for the specified users' access to devices. The default value is **Default schedule**. You can set a different schedule.

Select user or group window

In this window, you can specify a local or domain user or user group for which you want to configure an access rule.

Configuring an access rule

Setting	Description
Manual	If this option is selected, in the field below enter the name of the local or domain users or the

	name of a user group, to which the device access rule will apply.
List of groups or users	If this option is selected, in the search field you can enter search criteria for the name of the user or name of the user group, to which the device access control rule will apply, or you can select the name of the user group in the list below.

Schedules window

In this window, you can specify the schedule for the selected device access rule.

You can add, edit, and delete access schedule.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

You cannot delete the **Default schedule**.

Access schedule window

In this window, you can configure the device access schedule. You can configure schedules only for hard drives, removable drives, floppy disks, and CD/DVD drives.

In the **General settings** → **Application settings** section, if the **Block access to files during scans** check box is cleared, then it is not possible to block access to devices using an access schedule.

Schedule for access to devices

Setting	Description
Name	Entry field for the access schedule name. The schedule name must be unique.
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	This toggle switch sets the access mode for devices that use this bus: • **Allow** (default): provide access to devices connected through this bus. • **Block**: deny access to devices connected using this connection bus.

Configuring Device Control in the Administration Console

In the Administration Console, you can configure 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. The 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 a list of trusted devices by the device ID or by selecting it from the list of devices detected on the client 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 about detection of an attempt to access a device. • **Block** (default value). When this option is selected, Kaspersky Endpoint Security applies the access mode defined 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.

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	Name of a trusted device.
Device type	Trusted device type (for example, Hard drive or Smart card reader).
Host name	Host name the trusted device is connected to.
Comment	Comment related to a trusted device.

You can add a device to the list of trusted devices by ID or by mask or by selecting the required device in the list of devices detected on the user device.

You can edit and delete trusted devices in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

You can also import the list of devices from a file by clicking **Advanced** -> **Import** and export the list of added devices to a file by clicking **Advanced** -> **Export selected** or **Advanced** -> **Export all**. When importing, you will be prompted to replace the list of trusted devices or add the devices to the existing list.

Trusted device 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).

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 devices detected on client devices.

Information about existing devices is available only if there is an active policy and there has been synchronization with the Network Agent (performs within the limits specified in the Network Agent policy, 15 minutes by default). If you create a new policy and there are no other active ones, the list will be empty.

Adding device from list

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 the device with the specified settings. The search results are displayed in the table below.

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 options: • **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.

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	The list contains users and groups for which you can configure access schedule.

and/or user groups	By default, the table contains the **\Everyone** item (all users). You can add, edit, and delete users or user groups.
Schedule-based access rules for the selected user group	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, and delete access schedules for selected users. The **Default** schedule cannot be modified or removed. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table.

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	Name of the user or user group 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 options: • **Allow** (default): provide access to devices connected through this bus. • **Block**: deny access to devices connected using this connection bus.

Configuring Device Control on the command line

You can manage Device Control in the command line with the help of the Device Control predefined task (*Device_Control*).

The Device Control task runs by default. You can start and stop the task manually.

You can configure Device Control by editing the settings of the Device Control predefined task.

You can also view the list of connected devices using Device Control commands.

Device Control task settings

The table describes all available values and the default values of all the settings that you can specify for the Device Control task.

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 ap the access mode defined for t `Notify` – the application test access mode and generates a detection of an attempt to ac
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 ac `DependsOnBus` (default): acce drive depends on the access r the bus through which it is cor `Block` — Access to all hard dr hard drives, which are never bl Device Control) is blocked for `ByRule` — Access to the hard the access rules.
RemovableDrive	Access mode for the removable drives connected to a client device.	`Allow` — Access to the remov allowed for users. `DependsOnBus` (default): acce removable drive depends on t defined for the bus through w `Block` — Access to the remov blocked for users. `ByRule` — Access to the remo depends on the access rules.
FloppyDrive	Access mode for the floppy disks connected to a client device. The application does not block floppy disks connected to the client device using the ISA bus.	`Allow` — Users are allowed ac disks. `DependsOnBus` (default): acce disk depends on the access m bus through which it is connec `Block` — Access to floppy dis users. `ByRule` — Access to floppy d access rules.
OpticalDrive	Access mode for the CD/DVD drives connected to a client device.	`Allow` — Users are allowed ac drives. `DependsOnBus` (default): acce drive depends on the access r the bus through which it is cor `Block` — Access to CD/DVD users. `ByRule` — Access to CD/DVD the access rules.
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 ac connected through a serial po `DependsOnBus` (default): acce connected through a serial po access mode. `Block` — Access to devices c serial port is blocked for users
ParallelPortDevice	Access mode for the devices connected to a	`Allow` — Users are allowed ac connected through a parallel p

	client device via a parallel port.	`DependsOnBus` (default): acce connected through a parallel p bus access mode. `Block` — Access to devices c parallel port is blocked for use
Printer	Access mode for the printers connected to a client device.	`Allow` — Users are allowed ac `DependsOnBus` (default): acce depends on the access mode through which it is connected. `Block` — Access to printers is
Modem	Access mode for the modems connected to a client device.	`Allow` — Users are allowed ac `DependsOnBus` (default): acce depends on the access mode through which it is connected. `Block` — Access to modems i
TapeDrive	Access mode for the tape devices connected to a client device.	`Allow` — Users are allowed ac devices. `DependsOnBus` (default): acce depends on the access mode through which it is connected `Block` — Access to tape devi users.
MultifuncDevice	Access mode for the multifunctional devices connected to a client device.	`Allow` — Users are allowed ac multifunctional devices. `DependsOnBus` (default): acce multifunctional device depend mode defined for the bus thro connected. `Block` — Access to multifunc blocked for users.
SmartCardReader	Access mode for the smart card readers connected to a client device.	`Allow` — Access to smart car for users. `DependsOnBus` (default): acce reader depends on the access the bus through which it is cor `Block` — Access to smart car for users.
WiFiAdapter	Access mode for the Wi-Fi adapters connected to a client device.	`Allow` — Users are allowed ac adapters. `DependsOnBus` (default): acce adapter depends on connecti mode. `Block` — Access to the Wi-Fi for users.
NetworkAdapter	Access mode for the external network adapters connected to a client device.	`Allow` — Users are allowed ac network adapters. `DependsOnBus` (default): acce network adapter depends on t defined for the bus through w

		Device Control does not allo access to external network to avoid disconnecting the the network.
PortableDevice	Access mode for the portable devices connected to a client device.	`Allow` — Users are allowed ac devices. `DependsOnBus` (default): acce device depends on the access the bus through which it is cor `Block` — Access to portable d for users.
BluetoothDevice	Access mode for the Bluetooth devices connected to a client device.	`Allow` — Users are allowed ac devices. `DependsOnBus` (default): acce device depends on the access the bus through which it is cor `Block` — Access to Bluetooth for users.
ImagingDevice	Access mode for the imaging devices connected to a client device.	`Allow`—Access to all imaging for users. `DependsOnBus` (default): acce device depends on the access the bus through which it is cor `Block`—Access to all imaging for users.
SoundAdapter	Access mode for the sound adapters connected to a client device.	`Allow`—Access to all sound a for users. `DependsOnBus` (default): acce adapter depends on the acces the bus through which it is cor `Block`—Access to all sound a for users.
InputDevice	Access mode for the input devices (keyboards, mouse, touchpad, and others) connected to a client device.	`Allow` — Users are allowed ac devices. `DependsOnBus` (default): acce device depends on the access the bus through which it is cor `Block` — Access to input devi users.
The **[DeviceBus]** section contains access modes for connection buses.		
USB	Access mode for devices connected to the client device via USB.	`Allow` (default value) — Users to USB-devices. `Block` — Access to USB-devi users.
FireWire	Access mode for devices connected	`Allow` (default value) — Users to devices connected via the

	to the client device via FireWire.	`Block` — Access to devices c FireWire interface is blocked f
The **[TrustedDevices.item_ #]** section contains trusted devices.		
DeviceId	Specifies ID or ID mask of a trusted device.	You can use the masks * (any s characters) or ? (any single ch the device ID. Examples: *To deny access to all USB d specified one, specify the f* In the `[DeviceBus]` sectio `USB=Block` In the `[TrustedDevices.i` specify `DeviceId=<devic` *To deny access to all USB d access to all USB drives, sp following settings:* In the `[DeviceBus]` sectio `USB=Block` In the `[TrustedDevices.i` specify `DeviceId=USBSTO`
Comment	Comment to the specified trusted device.	—
The **[Schedules.item_#]** section contains the device access schedule. You can configure a schedule only for har drives, floppy disks, and CD/DVD drives.		
ScheduleName	Specifies a schedule name. The schedule name must be unique.	The default value: `Default`. The `Default` schedule provid to devices at any time if the c allowed to access the corresp You cannot delete the `Defaul`
DaysHours	Specifies time intervals for a schedule.	`All` (default value) — The sch (no time limitation). `< week_day >` — Days of the w either the full week day names (for example, for Monday, you `Mon`, or `Monday`). For week da intervals or specific days. The Sunday. `< hour >` — Hours [0:24]. You c intervals for hours. Examples: Schedule_1 is valid from Sun from 0 a.m. to 11 a.m., from 1 and from 4 p.m. to 12 a.m.:

		`[Schedules.item_0001]`
		`ScheduleName=schedule_`
		`DaysHours=Su-Sa:0..11`
		Schedule_2 is valid for the f
		on Thursdays from 12 p.m. to
		Fridays from 2 a.m. to 3 p.m.
		to 12 a.m.:
		`[Schedules.item_0002]`
		`ScheduleName=schedule_`
		`DaysHours=Th:12..14;Fr`
		Schedule_3 is valid 24 hours
		`[Schedules.item_0003]`
		`ScheduleName=schedule_`
		`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 schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or group, the n rights are granted.		
Principal	Specifies a user or group of users for whom the access rule is applied.	`\Everyone` (default value) — T applies to all users. `<user name>` — Name of the access rule applies. `@<group name>` — Name of to whom the access rule appli
[HardDrivePrincipals.item_#.AccessRules.item_#]	Access rule settings.	—
UseRule	Specifies whether the rule is enabled or disabled.	`Yes` (default value) — The acc `No` — The access rule is disabl
ScheduleName	Schedule specified in the [Schedules.item_#] section.	The default value: `Default`.
Access	Specifies access type.	`Allow` (default value) — Acces allowed. `Block` — Access to hard drive
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 rem multiple schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or gro access rights are granted.		
Principal	Specifies a user or group of users for whom the access rule is applied.	`\Everyone` (default value) — T applies to all users. `<user name>` — Name of the access rule applies. `@<group name>` — Name of to whom the access rule appli
[RemovableDrivePrincipals.item_#.AccessRules.item_#]	Access rule settings.	—

UseRule	Specifies whether the rule is enabled or disabled.	`Yes` (default value) — The acc `No` — The access rule is disabl
ScheduleName	Schedule specified in the [Schedules.item_#] section.	The default value: `Default`.
Access	Specifies access type.	`Allow` (default value) — Acce drives is allowed. `Block` — Access to removable
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 d schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or group, the n rights are granted.		
Principal	Specifies a user or group of users for whom the access rule is applied.	`\Everyone` (default value) — applies to all users. `<user name>` — Name of the access rule applies. `@<group name>` — Name of to whom the access rule appli
[FloppyDrivePrincipals.item_#.AccessRules.item_#]	Access rule settings.	—
UseRule	Specifies whether the rule is enabled or disabled.	`Yes` (default value) — The acc `No` — The access rule is disabl
ScheduleName	Schedule specified in the [Schedules.item_#] section.	The default value: `Default`.
Access	Specifies access type.	`Allow` (default value) — Acce is allowed. `Block` — Access to floppy dri
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/D multiple schedules can be specified for a user or group of users. If an access rule conflict occurs for a user or gro access rights are granted.		
Principal	Specifies a user or group of users for whom the access rule is applied.	`\Everyone` (default value) — applies to all users. `<user name>` — Name of the access rule applies. `@<group name>` — Name of to whom the access rule appli
[OpticalDrivePrincipals.item_#.AccessRules.item_#]	Access rule settings.	—
UseRule	Specifies whether the rule is enabled or disabled.	`Yes` (default value) — The acc `No` — The access rule is disabl
ScheduleName	Schedule specified	The default value: `Default`.

	in the [Schedules.item_#] section.	
Access	Specifies access type.	`Allow` (default value) — Acces drives is allowed. `Block` — Access to CD/DVD

Viewing a list of connected devices in the command line

Only users with the admin and audit roles can view the list of connected devices.

To view the list of connected devices, execute the following command:

```
kesl-control [-D] --get-device-list
```

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.

Web Control

Web Control controls user access to web resources. This allows you to reduce traffic consumption and reduce inappropriate use of working 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.

Kaspersky Endpoint Security monitors only HTTP and HTTPS traffic.

Web Control allows you to configure access to websites in the following ways:

- By content category. Website content is categorized based on Kaspersky Security Network, heuristic analysis, and a database of known websites (included in the application databases). You can restrict user access to, for example, the "Social networks" content category or other categories.
- By data type category. You can restrict user access to data on the website, and hide graphics, for example. The application determines the data type by the file format, not the extension.

  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.

- By web address. You can specify a web address or a web address mask.

You can use several methods to regulate access to websites at the same time. For example, you can restrict access to the "Office Application Files" data type only for the "Webmail" website category.

By default, the *default rule* selected for all web resources is **Allow**. In accordance with this rule, Web Control allows users to gain access to web resources if no other *web resource access rules* are defined.

You can change the default rule for Web Control, which governs how the application regulates access to web resources that are not covered by other rules, and set the *default rule* to **Block**. In accordance with this rule, Web Control prevents users from gaining access to web resources if no other *web resource access rules* are defined.

About web resource access rules

A *web resource access rule* is a set of filters and an action that the application performs when users visit web resources described in the rule at a time specified in the rule schedule. Filters let you specify web resources to which access is monitored by the Web Control component.

The following filters are available:

- **Filter by content category**. Web Control can categorize web resources based on content. You can control user access to web resources that have content defined by these categories. When users visit web resources that belong to a selected content category, the application performs the action specified in the rule.
- **Filter by data type category**. Web Control can categorize web resources based on data type. You can control user access to data located on web resources related to certain types of data. When users visit web resources that relate to a selected data type category, the application performs the action specified in the rule.
- **Filter by web resource address**. You can control user access to all addresses of a web resource or to individual addresses of a web resource and/or to groups of addresses of a web resource.

If you define both a filter by content category and/or data type category and a filter by web resource address, and the specified addresses of web resources and/or groups of web resource addresses belong to the selected content categories or data type categories, then the application does not control access to all of the web resources of the selected content categories and/or data type categories, but rather only controls access to the specified addresses of the web resources and/or groups of addresses of web resources.

- **Filter by name of users and user groups**. You can define users and/or user groups whose access to web resources is controlled according to the rule. For example, you can restrict browser access to the Internet for all users of an organization except the IT department.

- **Rule schedule**. You can set a 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 internet access through the browser access to working hours only.

For each rule, you can specify the action that Web Control performs when a user visits a web resource that matches the rule settings:

- *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.

- *Inform.* Web Control displays a warning that the web resource is undesirable. By clicking links in the warning message, the user can access the requested web resource.

Each rule has a priority. The higher the rule is on the list, the higher its priority. If a website is added to multiple rules, Web Control controls access to websites in accordance with the highest-priority rule. For example, the application may identify the corporate portal as a social network. To restrict access to social networks while allowing access to the corporate web portal, create two rules: a blocking rule for the "Social networks" category and an allowing rule for the corporate web portal. The corporate web portal access rule must have a higher priority than the social network access rule.

If no blocking rules are created, HTTPS traffic is not decrypted.

Configuring Web Control in the Web Console

In the Web Console, you can configure Web Control settings in the policy properties (**Application settings** → **Security Controls**→ **Web Control**)

Web Control component settings

Setting	Description
Web Control is enabled / disabled	This toggle switch enables or disables Web Control. This toggle switch is turned off by default.
List of rules	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: • **Rule name**. Web resource access rule name. • **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 enable or disable the toggle switch in the table, or 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. 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. This button is available if only one item is selected in the table. Clicking the **Move up** button moves the selected item up in the table. This button is available if only one item is selected in the table. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table. You can also import the list of rules from a file by clicking **Import** and export the list of added rules to a file by clicking **Export**. When importing, you will be prompted to replace the list of rules or add the rules to the existing list.
Default rule	You can select the default rule that governs how the application regulates access to web resources that are not covered by other rules: • **Allow everything not specified in the list of rules** (default) to allow access to web resources. • **Block everything not specified in the list of rules** to block access to web resources.
Templates	**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 input field contains the template for the message that appears when a rule is triggered that blocks access to a web resource. **Message 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. 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.

Web Control rule window

In this window, you can configure the settings of the web resource access rule.

Setting	Description
Rule name	Field for entering the name of the web resource access rule.
Status	You can select the 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.
Action	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.
Filter by content category	This check box enables or disables the content category filter. If the check box is selected, the **Content categories** link is available. Clicking this link opens a window in which you can select the relevant content categories. This check box is cleared by default.
Filter by data type category	This check box enables or disables the content category filter. If the check box is selected, the **Data type categories** link is available. Clicking this link opens a window in which you can select the relevant data type categories. This check box is cleared by default.
Addresses	You can select the way the web resource address filter is used: • **Apply to all addresses** (default). If this option is selected, the web resource address filter is not used; the Web Control rule is applied to all web resource addresses. • **Apply to the specified addresses and/or groups**. When this option is selected, the table of web resource addresses covered by the rule becomes available, as well as the **Add address** button, which you can click to open a window in which you can add the required address of the web resource, and the **Add group** button, which opens the **Address groups** window in which you can add groups of web resource addresses.
Users	You can select the way the user filter is applied for users that are covered by web resource access rules: • **Apply to all users** (default value). If this option is selected, the user filter is not used; the Web Control rule is applied to all users. • **Apply to the specified users and/or groups**. When this option is selected, the table of users and user groups covered by the rule becomes available, as well as the **Add** button, which opens the **Select user or group** window, in which you can add users and/or user groups.
Rule schedule	Web Control rule schedule. By default, **Always** is specified as the schedule. Clicking the **Always** link opens the **Schedules** window, in which you can configure a different schedule for the rule.

Address groups window

The table contains groups of addresses of web resources for which user access is controlled by the Web Control component. The table is empty by default.

Configuring a web resource access rule

Setting	Description
Group name	Name of the group of web resource addresses to which the rule applies.
Number of addresses in the group	Number of addresses in the address group.

You can add, edit, and 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 **Group** window by clicking the **Add** button above the table.

If you want to add a group of addresses to the list of groups in the **Web Control rule** window, select the check box next to a group name in the table and click the **Add groups to rule** button below the table.

Group window

In this window, you can add a group of web resource addresses.

Configuring a web resource access rule

Setting	Description
Group name	Name of the new group of web resource address group.
Addresses	Table of addresses included in the web resource address group.

You can add, edit, and delete items 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.

Select user or group

In this window, you can specify a local or domain user or user group for which you want to configure a web resource access rule.

Configuring a web resource access rule

Setting	Description
Manual	If this option is selected, in the field below enter the name of the local or domain users or the name of a user group to which the web resource access rule must apply.
List of groups or users	If this option is selected, in the search field you can enter search criteria for the name of the user or name of the user group to which the web resource access control rule must apply, or you can select the name of the user group in the list below.

Schedules window

In this window, you can specify the schedule for the selected device access rule.

You can add, edit, and delete access schedule.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The **Always** default schedule cannot be deleted or edited.

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. The schedule name must be unique.
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.

Configuring Web Control in the Administration Console

In the Administration Console, you can configure 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.
	Clicking the **Move down** button moves the selected item down in the table.
	This button is available if only one item is selected in the table.
	Clicking the **Move up** button moves the selected item up in the table.
	This button is available if only one item is selected in the table.
	Clicking the **Delete** button removes the selected item from the table.
	This button is available if at least one item is selected 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.
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. The 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 **Select content category** window. • **By data type category**. When this item is selected, the **Select** button becomes available. Clicking this button opens the **Select data type category** 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.
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.

Selecting the content category

In this window, you can select the content categories for which you want to control access.

To do so, select the check boxes next to the relevant categories.

All check boxes are cleared by default.

Selecting check boxes next to any nested content categories does not automatically select the check box next to the main content category that contains the nested categories.

Selecting the data type category

In this window, you can select the type categories for which you want to control access.

To do so, select the check boxes next to the relevant categories.

All check boxes are cleared by default.

Selecting addresses

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.

Selecting address groups

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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

If you want to add a new group of addresses to the list of groups in this window, open the **Add an address group** window by clicking the **Add** button above the table.

The table is empty by default.

Add an address group

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.

Selecting users

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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected 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.

Configuring Web Control message templates

Depending on the action specified in the properties of Web Control rules, when users attempt to access web resources, the application displays one of the following types of messages (by replacing the HTTP server response with an HTML page containing a message):

- Warning. This type of message warns the user that visiting the web resource is undesirable and/or violates the corporate security policy. The application displays a warning message if the **Inform** action is selected in the settings of the rule that matches this web resource.

  If the user believes the warning is a mistake, a link in the warning lets the user send an automatically-generated complaint message to the company's LAN administrator.

- Blocked web resource message The application displays a message that the web resource has been blocked (see the figure below) if the **Block** action is selected in the settings of the rule that matches this web resource.

  If the user believes the web resource should not be blocked, a link in the blocked web resource message lets the user send an automatically-generated complaint to the company's LAN administrator.

Templates are provided for warning messages, blocked web resource messages, and complaint messages to the company's LAN administrator. You can edit their content.

To change a message template in the Web Console:

1. In the main window of the Web Console, select **Assets (Devices)** → **Policies and policy profiles**.

   The list of policies opens.

2. Select the administration group containing the devices to which the policy is applied. To do so, click the link in the **Current path** field in the upper part of the window and select the administration group in the window that opens.

   The list displays the policies configured for the selected administration group.

3. Click the name of the required policy in the list.

   The policy properties window opens.

4. In the policy properties window, select **Application settings** → **Security Controls** → **Web Control**.

5. In the **Templates** section, 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 input field contains the template for the message that appears when a rule is triggered that blocks access to a web resource.

- **Message 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. 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.

6. Click **OK**.

7. Click the **Save** button to save the changes made.

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** → **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 input field contains the template for the message that appears when a rule is triggered that blocks access to a web resource.

   - **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 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.

7. Click **OK**.

8. Click **Apply**.

Configuring Web Control on the command line

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 settings

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 task settings

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 ac to the web resources. `Block` – block access to the we 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.	
`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 ac to the web resource. `Block` – block access to the we resource. `Notify` – display a warning that web resource is undesirable. By clicking links in the warning mess the user can access the request 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 W Control is running.
`ScheduleId`	Schedule ID that is used in the `[Schedules.item_#]` section.	
`UseUrls`	Use of a web resource	`Yes` – use a web resource addre

	address filter in a rule.	filter in the rule. No (default value) – do not use a resource address filter, apply th 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 th web resource address.
UseCategories	Use of filters by content categories and data type categories in the rule.	None (default) – do not use a w resource content filter. ContentOnly – use the conter category filter in the rule. FormatOnly – use the data typ category filter in the rule. ContentAndFormat – use the content category filter and the type category filter in the rule.
[Rules.item_#.ContentCategories.item_#]	Section for specifying the content category.	–
ContentCategory	Content categories.	AdultContent, AlcoholTobaccoNarcotics, Violence, Profanity, Weap ChatForum, WebMail, OnlineShops, SocialNets, Recruitment, HttpQueryRedirection, CreditCards, PoliceDecision, SoftwareAudioVideo, TechnologyElectronics, GamblingLotteriesSweepsta InternetCommunicationMedi CryptocurAndMining, LegislationBE, ECommerce, ComputerGames, Religions, News, Torrents, FileShari AudioAndVideo, BankSites, Blogs, DatingSites, LegislationR LegislationGlobal, SexuallyExplicit, Sexuality, GenerativeAITo
[Rules.item_#.FormatCategories.item_#]	Section for specifying the data type category.	–
FormatCategories.item_#.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 r `No` (default value) – do not use t user filter, apply the rule to all us
`[Rules.item_#.Principals.item_#]`	Section for specifying users that are covered by the web resource access rule.	
`isGroup`	This setting specifies whether the name specified in the `Name` field is a user name or a group name.	`Yes` – The specified name is a g name. `No` – The specified name is a us name.
`Name`	User or group of users that is covered by the web resource access rule.	`<user name>`: name of the use whom the rule applies. `@<group name>`: name of the of users to whom the rule applie
`Sid`	The ID of the user or user group.	
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 th web resource address.
The **[Schedules.item_#]** section contains the rule schedule.		
`Id`	Schedule ID that is used in the `[Rules.item_#]` section.	`1 to 999999` `0` is the ID of the `Default` sche which lets the rule work without time limits, that is, at all times.
`Name`	Specifies a schedule name.	
`DaysHours`	Specifies time intervals for a schedule.	`<week_day>` — Days of the we You can use either the full week names or abbreviations (for exa for Monday, you can specify `Mo` `Mon`, or `Monday`). For week days can specify intervals or specific The week starts from Sunday.

		< hour > — Hours [0:24]. You ca 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 configuration file>] [--json]
```

where:

`--file <path to configuration file>` – full path to the configuration file to which the settings will be exported.

`--json`: output data in JSON format.

To edit Web Control settings, run the following command:

```
kesl-control --set-settings 26 [--file <path to configuration file>] [--json]
```

where:

`--file <path to configuration file>` – full path to the configuration file from which the settings will be imported.

`--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
```

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.
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.

System Integrity Monitoring

Kaspersky Endpoint Security monitors the integrity of the operating system on the protected device in real time or on demand.

- *System Integrity Monitoring* tracks in real time changes in files and directories that you have added to the monitoring scope in the component settings. You can track changes in files that may indicate a security breach on a protected device.
- You can use the *System Integrity Check* tasks to check for changes in files and directories that you have added to the monitoring scope by comparing the current state of a monitored object with a previously recorded state.

Using System Integrity Monitoring requires a license that includes this feature.

This feature is not supported in the KESL container.

Upon detecting changes to files or directories in the monitoring scope, Kaspersky Endpoint Security generates events about changes in object access control lists. 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.

Real-time System Integrity Monitoring

System Integrity Monitoring detects each change to an object within the monitoring scope by intercepting file operations in real time.

When System Integrity Monitoring runs, the application monitors changes in the following file settings:

- Content (write (), truncate (), etc.)
- Metadata (possession rights (chmod/chown))
- Time stamps (utimensat)
- Extended attributes ((setxattr) and others)

A file checksum is not calculated.

The technical limitations of the Linux operating system prevent the application from identifying the user or process that made the changes to the file.

System Integrity Monitoring is disabled by default. You can enable, disable, and configure System Integrity Monitoring:

- Define monitoring scopes for System Integrity Monitoring The application monitors operations on files within the monitoring scopes defined in the System Integrity Monitoring settings. You have to specify at least one monitoring scope for the component to work. The *Kaspersky internal objects* (/opt/kaspersky/kesl/) monitoring scope is defined by default.

  You can specify several monitoring scopes. You can change monitoring scopes in real-time mode.

The application task does not monitor changes in files (attributes and content) with hard links that are outside the monitoring scope.

- You can configure exclusion of objects from monitoring with the help of name masks.
- Set up exclusion scopes for System Integrity Monitoring. Exclusions are defined for each individual monitoring scope and only work for the indicated scope. You can specify several monitoring exclusions.

  An exclusion has a higher priority than a monitoring scope; an excluded object is skipped even if within the 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.

When a directory is added to a monitoring or exclusion scope, the application does not check whether that directory exists.

Configuring System Integrity Monitoring in the Web Console

In the Web Console, you can configure System Integrity Monitoring settings in the policy properties (**Application settings** → **Security Controls**→ **System Integrity Monitoring**).

System Integrity Monitoring settings

Setting	Description
System Integrity Monitoring enabled / disabled	This toggle switch enables or disables the System Integrity Monitoring component. The toggle button is switched off by default.
Monitoring scopes	Clicking the **Configure monitoring scopes** link opens the **Monitoring scopes** window.
Exclusion scopes	Clicking the **Configure monitoring** exclusion scopes link opens the **Exclusion scopes** window.
Exclusions by mask	Clicking the **Configure exclusions by mask** link opens the **Exclusions by mask** window.

Monitoring 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 the **Kaspersky internal objects** (/opt/kaspersky/kesl/) monitoring scope.

Monitoring scope settings for System Integrity Monitoring

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.

Clicking the **Move down** button moves the selected item down in the table.

This button is available if only one item is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

This button is available if only one item is selected in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Add monitoring scope window

In this window, you can add and configure monitoring scope for the System Integrity Monitoring component.

Monitoring scope settings

Setting	Description
Scope name	Field for entering the monitoring scope name. This name will be displayed in the table in the **Monitoring 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 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. The 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.

	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. The **/** path is specified by default – the application scans all directories of the local file system.
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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Exclusion scopes window

The table 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. By default, the table is empty.

Monitoring exclusion scope settings

Setting	Description
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.

You can add, edit, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Add 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. The 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.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. 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 **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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 **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

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).

Configuring System Integrity Monitoring in the Administration Console

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
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.

Clicking the **Move down** button moves the selected item down in the table.

This button is available if only one item is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

This button is available if only one item is selected in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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 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. The 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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Exclusion scopes window

The table 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. By default, the table is empty.

Monitoring exclusion scope settings

Setting	Description
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.

You can add, edit, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

<Exclusion scope name> 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. The 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 **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table. The selected element's settings are changed in a separate window. 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 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 **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

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).

Configuring System Integrity Monitoring in the command line

You can manage system integrity monitoring in real time in the command line by using the System Integrity Monitoring predefined task (*System_Integrity_Monitoring*). Task type: *OAFIM*.

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.

On-access File Integrity Monitoring task settings

Setting	Description	Values
`UseExcludeMasks`	Enables monitoring scope exclusions for objects specified by the `ExcludeThreats.item_#` setting. This setting only applies if a value is specified for the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from the monitoring scope. `No` (default value) — Do not exclude 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. 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. 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. 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. 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)

System Integrity Check

When the *System Integrity Check* task is running, a change in each object is found by comparing the current state of the monitored object with its original state. The following comparison criteria can be used:

- File hash
- File change time
- File size

The initial state of monitored objects is recorded as a *baseline*. The baseline contains paths to monitored objects and their metadata.

A baseline may also contain personal data.

A system baseline is created when a System Integrity Check task runs on the device for the first time. If you have created multiple System Integrity Check tasks, a separate baseline is created for each. The task is only executed if the baseline contains information about objects that belong to the monitoring scope defined for the task. If the baseline does not match the monitoring scope, Kaspersky Endpoint Security generates a system integrity violation event.

A baseline is rebuilt when task settings change, for example, if a new monitoring scope is added.

The application creates a baseline storage on the protected device. By default, 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.

You can delete a baseline by deleting the appropriate System Integrity Check task.

You can run a system integrity check on demand and configure the scan settings:

- Enable or disable baseline rebuild every time a system integrity check task finishes.
- Select criteria for comparing the current state of the monitored file with the original state: use the file hash and change time, or only the file size.
- Configure monitoring scopes for checking system integrity.
- Configure exclusion scopes from the system integrity check. You can specify paths to excluded files and directories, and exclude individual objects by name mask.

Configuring System Integrity Check in the Web Console

You can run a system integrity check in the Web Console with the help of the *System Integrity Check* task.

You can create and run user system integrity check tasks. You can configure the scan settings by editing the settings of the tasks.

System Integrity Check task settings

Setting	Description
Rebuild baseline on each task start	This check box enables or disables the reestablishment of a system baseline upon every start of the *System Integrity Check* task. 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 checkbox 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 directory monitoring while system integrity check is running. 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 monitoring runs. This check box is cleared by default.
Monitoring scopes	The table that contains the monitoring scopes scanned by the task. By default, the table contains the **Kaspersky internal objects** (/opt/kaspersky/kesl/) monitoring scope. You can add, configure, delete, move up, or move down monitoring scopes 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. Clicking the scan scope name opens the **<Scan scope name>** window. In this window, you can modify the settings of the selected scan scope.

Clicking the **Add** button opens the **<New scan scope>** window. In this window, you can define a new scan scope.

Add scan scope window

In this window, you can add or configure monitoring scopes for the System Integrity Check task.

Monitoring scope settings

Setting	Description
Scope name	Field for entering the monitoring scope name. This name will be displayed in the table in the **Scan settings** section. 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. The 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. 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. The field must not be blank. The **/** path is specified by default – the application scans all directories of the local file system.
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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Exclusion scopes section

In the **Exclusion scopes** section, you can configure exclusion scopes and exclusions by mask for the System Integrity Check task.

Exclusion scopes window

The table contains monitoring exclusion scopes for the System Integrity Check task. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

Monitoring exclusion scope settings

Setting	Description
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 task operation.

You can add, edit, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

Add exclusion scope window

In this window, you can add and configure the monitoring exclusion scope for the System Integrity Check task.

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. The 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. 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. 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 **Delete** button removes the selected item from the table. This button is available if at least one item 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.

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 **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

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).

Configuring System Integrity Check in the Administration Console

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 user system integrity check tasks. You can configure the 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 reestablishment of a system baseline upon every start of the System Integrity Check task. 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 checkbox 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	This check box enables or disables scanning of directories within the specified

in monitoring scopes	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 monitoring 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.

Under **Exclusion scopes** 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.

Clicking the **Move down** button moves the selected item down in the table.

This button is available if only one item is selected in the table.

Clicking the **Move up** button moves the selected item up in the table.

This button is available if only one item is selected in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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 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. The 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. 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. 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. Clicking the **Delete** button removes the selected item from the table. This button is available if at least one item 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.

Exclusion scopes 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 monitoring exclusion scopes for the System Integrity Check task. The application does not scan files and directories located at the paths specified in the table. By default, the table is empty.

Monitoring 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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item 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.

<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. The 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. 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. 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 **Delete** button removes the selected item from the table. This button is available if at least one item is selected in the table. The selected element's settings are changed in a separate window.

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 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 **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

The selected element's settings are changed in a separate window.

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).

Configuring System Integrity Check in the command line

You can run a system integrity check on a device in the command line by using user *System Integrity Check* tasks (*ODFIM* tasks).

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 the last time a file was accessed. `No` (default value) — Do not track the last time a file was accessed.
`UseExcludeMasks`	Enables monitoring scope exclusions for objects specified by the `ExcludeMasks.item_#` setting. This setting only applies if a value is specified for the `ExcludeMasks.item_#` setting.	`Yes` — Exclude objects specified by the `ExcludeMasks.item_#` setting from the monitoring scope. `No` (default value) — Do not exclude 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.
`Path`	Path to the monitoring directory.	You can use masks to specify the path. 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. 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. 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. 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)

Behavior Detection

The Behavior Detection component allows you to monitor for any malicious activity from applications in the operating system. When malicious activity is detected, Kaspersky Endpoint Security can terminate the process of the application that performs malicious activity.

This feature is not supported in the KESL container.

The Behavior Detection component is enabled automatically with the default settings when Kaspersky Endpoint Security starts.

You can enable, disable, and configure Behavior Detection:

- Select an action to be performed by Kaspersky Endpoint Security upon detecting malicious activity in the operating system: inform the user or block the application that performs malicious activity.
- Exclude process activity from scans.

If integration between Kaspersky Endpoint Security and Kaspersky Managed Detection and Response is enabled, exclusions by process are skipped when detecting application behavior in the operating system.

By default, on the SintezM-Client operating system, the auditd service configuration is protected from modification, 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.

Configuring Behavior Detection in the Web Console

In the Web Console, you can configure Behavior Detection settings in the policy properties (**Application settings** → **Advanced Threat Protection** → **Behavior Detection**).

Behavior Detection setting

Setting	Description
Behavior Detection enabled / disabled	This toggle switch enables or disables the Behavior Detection component. The check toggle button is switched on by default.
Action on malware activity detection	The action to be performed by Kaspersky Endpoint Security upon detecting malicious activity in the operating system: • **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. • **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.
Exclusions by	Clicking the **Configure exclusions by process** link opens the **Exclusions by process**

process	window. In this window, you can exclude the activity of processes.

Exclusions by process window

The table contains the exclusion scopes for exclusion by process The exclusion scope for exclusion by process lets you exclude the activity of the indicated process and files modified by the indicated process. By default, the table is empty.

If integration between Kaspersky Endpoint Security and Kaspersky Managed Detection and Response is enabled, exclusions by process are not applied.

Exclusion scope settings for exclusion by process

Setting	Description
Exclude / Do not exclude trusted processes from scans	The switch enables or disables the configured exclusions by process in the operation of the Behavior Detection component. The toggle button is switched off 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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

You can also import the list of exclusions from a file by clicking **Import** and export the list of added exclusions to a file by clicking **Export**. When importing, you will be prompted to replace the list of exclusions or add the exclusions to the existing list.

Adding a process exclusion scope window

In this window, you can add and configure exclusion scopes for exclusion by process.

Exclusion scope settings

Setting	Description
Process-based exclusion scope name	Field for entering the Process-based exclusion scope name. This name will be displayed in a table in the **Exclusions by process** window. The entry field must not be blank.
Use this exclusion	This check box enables or disables this scan scope exclusion when the application is running. The check box is selected by default.
Path to excluded	Full path to the process you want to exclude from scans. You can use masks to specify the path.

process	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. 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.

Configuring Behavior Detection in the Administration Console

In the Administration Console, you can configure Behavior Detection settings in the policy properties (**Advanced Threat Protection → Behavior Detection**).

Behavior Detection setting

Setting	Description
Enable Behavior Detection	This check box enables or disables the Behavior Detection component. The 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

The table contains the exclusion scopes for exclusion by process The exclusion scope for exclusion by process lets you exclude the activity of an indicated process. By default, the table is empty.

If integration between Kaspersky Endpoint Security and Kaspersky Managed Detection and Response is enabled, exclusions by process are not applied.

Exclusion scope settings for exclusion by process

Setting	Description
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, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected 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**. When importing, you will be prompted to replace the list of exclusions or add the exclusions to the existing list.

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.

	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. 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. The check box is selected by default.

Configuring Behavior Detection in the command line

You can manage application Behavior Detection in the operating system via the command line by using the *Behavior_Detection* predefined task.

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
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.
UseTrustedPrograms	Excluding processes from scans.	Yes – do not scan the activity of the indicated processes. No (default value) – scan all processes.
The **[TrustedPrograms.item_#]** section contains processes that are excluded from 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 indicated local directory. You can use masks to specify the path. 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.
`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`	Enables the exclusion of the specified process from scanning.	`Yes` (default value) - enable exclusion of the specified process from scanning. `No` - do not exclude the specified process from scanning.

Using Kaspersky Security Network

To increase the protection of devices and user data, Kaspersky Endpoint Security can use Kaspersky's cloud-based knowledge base Kaspersky Security Network (KSN) to check the reputation of files, Internet resources, and software. Using Kaspersky Security Network data ensures a faster response to various threats, high protection component performance, and fewer false positives.

Use of Kaspersky Security Network is voluntary. You can start or stop using KSN at any time.

This feature is not supported in the KESL container.

Kaspersky Security Network infrastructure solutions

Kaspersky Endpoint Security supports the following infrastructure solutions to work with Kaspersky reputation databases:

- *Kaspersky Security Network (KSN)* – A solution that receives information from Kaspersky and sends data about objects detected on user devices to Kaspersky for additional verification by Kaspersky analysts and to add to reputation and statistical databases.
- *Kaspersky Private Security Network (KPSN)* – A solution that allows users of devices with Kaspersky Endpoint Security installed to access the reputation databases of Kaspersky, as well as other statistical data, without sending data to Kaspersky from their devices. KPSN is designed for corporate clients who can't use Kaspersky Security Network, for example, for the following reasons:
  - No connection of local workplaces 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 a new application license, inform the service provider about the new license key. Otherwise, an authentication error will prevent data exchange with KPSN.

Kaspersky Security Network usage options:

There are two options for using KSN:

- **Extended KSN mode** – you can receive information from the Kaspersky knowledge base, while Kaspersky Endpoint Security automatically sends statistical information to Kaspersky Security Network that it obtained during its operation. The application can also send to Kaspersky for additional scanning certain files (or parts of files) that intruders can use to harm the device or data.
- **Basic KSN mode** – you can receive information from the Kaspersky knowledge base, but Kaspersky Endpoint Security does not send anonymous statistics and data about the types and sources of threats.

You can select a different Kaspersky Security Network usage option at any time.

No personal data is collected, 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 website. The file with the text of the Kaspersky Security Network Statement is included in the application distribution kit.

Cloud mode for Kaspersky Endpoint Security

Cloud mode is an operating mode of Kaspersky Endpoint Security that uses a lightweight version of the malware databases. This lets you reduce the load on device memory.

Kaspersky Security Network facilitates the application's use of the lightweight malware databases.

You can enable cloud mode if Kaspersky Endpoint Security is running in standard mode and using KSN.

Lightweight anti-malware databases are not supported if Kaspersky Endpoint Security is running in Light Agent mode for protecting virtual environments. The application receives special databases required for Light Agent operation from Protection Server.

Kaspersky Endpoint Security switches to using a lightweight version of the malware databases after enabling cloud mode and performing the latest update of the application databases and modules. If cloud mode is disabled, Kaspersky Endpoint Security downloads the full version of the application databases from Kaspersky servers during the next update of application databases and modules.

If you are not using KSN or cloud mode is disabled, Kaspersky Endpoint Security uses the full version of the application databases.

Cloud mode is disabled automatically if use of KSN is disabled.

Using the KSN Proxy service

User devices managed by Administration Server can communicate with KSN directly or via the KSN Proxy service.

If Kaspersky Endpoint Security is running in Light Agent mode to protect virtual environments, the KSN Proxy service supports communication with the KSN infrastructure. Direct communication with KSN is not supported. If the KSN proxy is not available, KSN is not used by the application.

A KSN proxy server provides the following capabilities:

- The user's device can query KSN and submit information to KSN, even without direct access to the Internet.
- A KSN proxy server caches processed data, thereby reducing the load on the external network connection and speeding up receipt of the information that is requested by the user's device.

The KSN proxy server settings can be configured in the Administration Server properties. For details about the KSN proxy server, refer to the Kaspersky Security Center Help.

Configuring the use of Kaspersky Security Network in the Web Console

In the Web Console, you can configure the use of Kaspersky Security Network in Kaspersky Endpoint Security in the policy properties (**Application settings** → **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 **Assets (Devices)** tab.

Kaspersky Security Network settings

Setting	Description
Do not use KSN	By selecting this option, you decline to use Kaspersky Security Network.
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 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.
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 online knowledge base about the reputation of files, web resources, and software.
Enable cloud mode	The check box enables or disables the operating mode in which Kaspersky Endpoint Security uses a lightweight version of the malware databases. 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 KSN servers when KSN Proxy is not available	The check box enables or disables the ability to communicate with KSN servers directly when the KSN Proxy service is unavailable. The check box is selected by default. This setting applies only if the application is used in Standard mode.
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.
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.

Configuring the use of Kaspersky Security Network in the Administration Console

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	The check box enables or disables the operating mode in which Kaspersky Endpoint Security uses a lightweight version of the malware databases. 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 KSN servers when KSN Proxy is not available	The check box enables or disables the ability to communicate with KSN servers directly when the KSN Proxy service is unavailable. The check box is selected by default. 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 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 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.

Configuring the use of Kaspersky Security Network in the command line

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 `UseKSN` with the help of command line switches 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`: a key 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 <configuration file name> [--json] [--accept-ksn]
```

where:

- `--file <the path to the configuration file>`: the full path to the configuration file with the general application settings where the required `UseKSN` value is set.
- `--json`: specify this key if you are importing settings from a configuration file in JSON format. If the `--json` key is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.
- `--accept-ksn`: a key signifying that you agree to the terms in the Kaspersky Security Network Statement. You have to specify the key if enabling the use of Kaspersky Security Network.

If Kaspersky Endpoint Security installed on a client device runs under a policy that was assigned in Kaspersky Security Center, 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`.

Checking the connection to Kaspersky Security Network using the command line

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 `Extended KSN mode` 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 `Basic KSN mode` 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 status is `Disabled`, 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: `Kaspersky Security Network` or `Kaspersky Private Security Network`.

A connection to Kaspersky Security Network may be absent for the following reasons:

- The user device is not connected to the internet.
- Using 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 and disabling cloud mode from the command line

Cloud mode is an operating mode of Kaspersky Endpoint Security that uses a lightweight version of the malware databases.

Lightweight anti-malware databases are not supported if Kaspersky Endpoint Security is running in Light Agent mode for protecting virtual environments. 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 value of `CloudMode` using a configuration file that contains all general application settings or with command line options.

Cloud mode is available if use of Kaspersky Security Network is enabled.

Advanced application settings

You can configure the following additional application settings:

- Using a proxy server in the application.
- Global exclusions – exclude mount points from file operation interception for the File Threat Protection, Anti-Cryptor, and Container Monitoring components and the Critical Areas Scan, Container Scan, and Removable Drives Scan tasks.
- Exclude process memory from scans.
- File operations interception mode.
- Detection of legitimate applications that threat intruders can use to compromise devices or data.
- Application stability monitoring.
- Application startup settings.
- Limit on the use of memory and processor resources for scan tasks.
- Limit on the use of resident memory by the application.
- Limit on the number of Custom Scan tasks that a non-privileged user can start simultaneously.
- Settings for forwarding of information to the Kaspersky Security Center storage.
- Task management permissions.

Configuring a proxy server

You can configure proxy server settings if the users of the client devices use a proxy server to connect to the internet. Kaspersky Endpoint Security may use a proxy server to connect to Kaspersky servers, for example, when updating application databases and modules or when communicating with Kaspersky Security Network and Kaspersky Endpoint Detection and Response (KATA).

The proxy server is disabled by default.

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.

Configuring proxy server settings in the Web Console

In the Web Console, you can configure use of a proxy server in the policy properties (**Application settings** → **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.
Specify the proxy server settings	If this option is selected, the application uses the specified proxy server settings, for example, for integration with Kaspersky Endpoint Detection and Response (KATA).
Address	Field for entering the proxy server's IP address or domain name. This field is available if the **Use the specified proxy server settings** option is selected.
Port	Field for entering the proxy server's port. Default value: 3128. This field is available if the **Use the specified proxy server settings** option is selected.
Use proxy server authentication	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.
Edit	Allows you to specify a password for authenticating on the proxy server. The **Password** field cannot be edited. By default, the password is empty. To specify a password, click **Edit**. In the window that opens, enter the password and click **OK**. 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 in the window displays the password in clear text in the password entry window. The button is available if the **Use proxy server authentication** check box is selected.
Use Kaspersky Security Center as a proxy server for application activation	This check box enables or disables use of Kaspersky Security Center as a proxy server for application activation. If this check box is selected, Kaspersky Endpoint Security uses Kaspersky Security Center as a proxy server for the application activation. 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 to protect virtual environments, the license information is provided by the Protection Server.

Configuring proxy server settings in the Administration Console

In the Administration Console, you can configure the use of a proxy server 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.
Specify the proxy server settings	If this option is selected, the application uses the specified proxy server settings, for example, for integration with Kaspersky Endpoint Detection and Response (KATA).
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.
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	This check box enables or disables use of Kaspersky Security Center as a proxy server for application activation. If this check box is selected, Kaspersky Endpoint Security uses Kaspersky Security Center as a proxy server for the application activation. 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 to protect virtual environments, the license information is provided by the Protection Server.

Configuring proxy server settings in the command line

You can enable or disable the use of a proxy server by application components in the command line with the help of the `UseProxy` and `ProxyServer` settings in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

The `UseProxy` setting can take the following values:

- `Yes` - enable the use of a proxy server.
- `No`: disable the proxy server.

The `ProxyServer` setting lets you define proxy server settings in the format: `[<user>[:<password>]@]<proxy server address>[:<port>]`, where:

- `<user>` is a user name for proxy server authentication.
- `<password>` is a user password for proxy server authentication.
- `<proxy server address>` is the proxy server IP address or domain name.
- `<port>` is the proxy server port.

If no authentication is required for connecting to the proxy server, you do not need to define `ProxyServer`.

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.

Configuring global exclusions

You can configure exclusion of mount points from file operation interception for the File Threat Protection and Anti-Cryptor components, as well as from scanning by the Malware Scan, Critical Areas Scan, and Container Scan tasks. Exclusion of mount points allows you to exclude local or remote directories mounted on a device from interception of file operations. In addition, global exclusions affect the operation of the Container Monitoring component and the Removable Drives Scan task.

Configuring global exclusions in the Web Console

In the Web Console, you can configure use of global exclusions in the policy properties (**Application settings** → **General settings** → **Global exclusions**).

The table in the **Global exclusions** section contains mount points to be excluded from file operation interception.

The **Path** column displays the paths to the excluded mount points. The table is empty by default.

You can add, edit, and delete items in the table.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

Adding a mount point exclusion window

Mount point settings

Setting	Description
File system, access protocol, and path	In this drop-down list, 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.
Access protocol	You can select the remote access protocol in the drop-down list: • **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. This drop-down list is available if the **Mounted** type is selected in the drop-down list of file systems.
Path	Field for entering the path to the mount point that you want to exclude from file operation interception. You can use masks to specify the path.

	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. To exclude the mount point /dir, you need to specifically indicate /dir (no asterisk). The mask /dir/* excludes all mount points at the level below /dir but not /dir itself. The /dir/** mask excludes all mount points below the level of /dir but not /dir itself. You can use a single ? character to represent any one character in the file or directory name. This field is available if the **Local** type is selected in the drop-down list of file systems.
Name of shared resource	The field for entering the name of the file system shared resource, where the directories that you want to add to the file operation interception exclusions are located. The field is available if the **Mounted** type is selected in the File system drop-down list and the **Custom** item is selected in the **Access protocol** drop-down list.

Configuring global exclusions in the Administration Console

In the Administration Console, you can configure use of 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.

Clicking the **Delete** button removes the selected item from the table.

This button is available if at least one item is selected in the table.

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. 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. To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk). The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself. You can use a single `?` character to represent any one character in the file or directory name.
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.

Configuring global exclusions in the command line

You can define mount point exclusions in the command line via the `ExcludedMountPoint.item_#` option in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

The `ExcludedMountPoint.item_#` option accepts 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 that contains the /mnt/user* or /mnt/**/user_share>` — Exclude objects in mount points whose names contain the specified mask from file operation interception.

  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.

  To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk).

  The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself.

  You can use a single ? character to represent any one character in the file or directory name.

You can specify several mount points to exclude from scanning.

Mount points must be specified in the same way as they are displayed in the `mount` command output.

Exclude process memory from scans

You can exclude process memory from scans. The application does not scan the memory of the specified processes.

Configuring exclusions in the Web Console

In the Web Console, you can configure excluding process memory from scans in the policy properties (**Application settings** → **General settings** → **Application settings**).

Clicking **Configure exclusion of process memory from scans** under **Exclude process memory from scans** opens the **Exclude process memory from scans** 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 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.

To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk).

The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself.

You can use a single ? character to represent any one character in the file or directory name.

You can add, edit, and delete items in the list.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected process path from the list.

This button is available if at least one process path is selected in the list.

The **Edit** button a window where you can change the process path. Kaspersky Endpoint Security excludes the memory of the indicated process from scans.

The **Add** button opens a window where you can enter the full path to a process. Kaspersky Endpoint Security excludes the memory of the indicated process from scans.

Configuring exclusions in the Administration Console

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 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.

To exclude the mount point `/dir`, you need to specifically indicate `/dir` (no asterisk).

The mask `/dir/*` excludes all mount points at the level below `/dir` but not `/dir` itself. The `/dir/**` mask excludes all mount points below the level of `/dir` but not `/dir` itself.

You can use a single ? character to represent any one character in the file or directory name.

You can add, edit, and delete items in the list.

Clicking the **Delete** button causes Kaspersky Endpoint Security to remove the selected process path from the list.

This button is available if at least one process path is selected in the list.

The **Edit** button a window where you can change the process path. Kaspersky Endpoint Security excludes the memory of the indicated process from scans.

The **Add** button opens a window where you can enter the full path to a process. Kaspersky Endpoint Security excludes the memory of the indicated process from scans.

Configuring exclusions 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 edit the setting using command line options 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 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.

You can specify several processes to exclude from scanning.

Selecting the interception mode for file operations

The file operation interception mode affects the File Threat Protection and Device Control components.

- For the duration of the scan, the application can block access to files that are being scanned by the File Threat Protection component. By default, access is blocked: any access to the scanned file must wait until the scan results are in. If the scan detects no threats in the file, the application allows access to the file. When detecting infected objects, the application takes the actions specified in the **First action** (`FirstAction`) and **Second action** (`SecondAction`) settings for File Threat Protection.

  You can choose not to block access to files that are being scanned by the File Threat Protection component. In that case, the scan is performed asynchronously.

- 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. By default, access is blocked: any access to files on the managed device must wait until the scan results are in. The application allows access to files if after the scan, Device Control allows access to the device that contains the files.

  You can disable file access blocking on the device monitored by the Device Control component. In that case, Device Control determines if access to the device can be allowed in asynchronous mode.

Configuring in the Web Console

In the Web Console, you can configure the file operation interception mode in the policy properties (**Application settings** → **General settings** → **Application settings**, **File operation interception mode** section).

The **Block access to files during scans** 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 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.

Configuring in the Administration Console

In the Administration Console, you can configure the file operation interception mode in the policy properties (**General settings** → **Application settings**, **File operation interception mode** section).

The **Block access to files during scans** 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 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.

Configuring in the command line

You can configure the file operation interception mode in the command line using the `FileBlockDuringScan` setting in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

The `FileBlockDuringScan` option accepts the following values:

- `Yes` (default value) to block access to files for the duration of the scan by the File Threat Protection and Device Control components.
- `No` to allow access to files during the scan. Requests to any file is allowed, scanning is done asynchronously.

  This file operation interception mode has less impact on the system performance, but there is a risk that a threat in a file will not be disinfected or deleted if the file can, for example, change its name during a scan before the application makes a decision on the status of the file.

Configuring detection of applications that hackers can use to harm

You can enable or disable detection of legitimate applications that intruders can use to compromise devices or data.

Configuring in the Web Console

In the Web Console, you can detection of legitimate applications that intruders can use to compromise devices or data in the policy properties (**Application settings** → **General settings** → **Application settings**, **Scan settings** section).

The **Detect legitimate applications that intruders can use to compromise devices or data** check box enables or disables detection of legitimate applications that intruders can use to compromise the device or data of the user.

This check box is cleared by default.

Configuring in the Administration Console

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).

The **Detect legitimate applications that intruders can use to compromise devices or data** check box enables or disables detection of legitimate applications that intruders can use to compromise the device or data of the user.

This check box is cleared by default.

Configuring in the command line

In the command line, you can enable or disable detection of legitimate applications that intruders can use to compromise devices or data by using the `DetectOtherObjects` setting in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

`DetectOtherObjects` accepts the following values:

- `Yes`: enable detection of legitimate applications that intruders can use to compromise devices or data.
- `No`: do not enable detection of legitimate applications that intruders can use to compromise devices or data.

Enabling application stability monitoring

You can enable or disable the Kaspersky Endpoint Security stability monitoring that lets you track the number of times the application terminates abnormally and notify the administrator about the unstable operation of the application.

Configuring in the Web Console

In the Web Console, you can enable or disable application stability monitoring in the policy properties (**Application settings** → **General settings** → **Application settings**, **Advanced application settings** section).

The **Enable application stability monitoring** check box enables or disables monitoring of the state of the Kaspersky Endpoint Security application.

This check box is cleared by default.

To apply the setting, you must restart the application.

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>*.

Configuring in the Administration Console

In the Administration Console, you can enable or disable application stability monitoring in the policy properties (**General settings** → **Application settings**, **Advanced application settings** section).

The **Enable application stability monitoring** check box enables or disables monitoring of the state of the Kaspersky Endpoint Security application.

This check box is cleared by default.

To apply the setting, you must restart the application.

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>*.

Configuring in the command line

In the command line, you can configure application stability monitoring using the `TrackProductCrashes`, `ProductHealthLogFile`, `WarnThreshold`, `WarnAfter_#_crash` and `WarnRemovingThreshold` settings in the kesl.ini configuration file.

The `TrackProductCrashes` setting lets you enable or disable application stability monitoring. This setting can take the following values:

- `Yes/true` – enable application stability monitoring.
- `No/false` – do not enable application stability monitoring.

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 that are required before displaying a notification about unstable application operation. The setting can take values from 0 to 10. Default value: 10. If the value is 0, an unstable application notification is not displayed.

Configuring application startup settings

You can configure the application startup settings.

Setting a limit in the Web Console

In the Web Console, you can configure the application startup settings in the policy properties (**Application settings** → **General settings** → **Application settings**, **Application startup settings** section).

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.

Setting a limit in the Administration Console

In the Administration Console, you can configure the 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.

Setting a limit 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.

Limiting the use of memory and processor resources

You can set a limit on CPU usage for scan tasks. No limit is set by default. You can also configure memory usage limits for scan tasks. The default limit is 8192 megabytes.

Setting a limit in the Web Console

In the Web Console, you can enable and disable the CPU utilization limit and configure the memory usage limit for scan tasks in the policy properties (**Application settings** → **General settings** → **Application settings**, **Performance** section).

Settings

Setting	Description
Memory usage limit for scan tasks (MB)	Input field for the memory usage limit for scan tasks (in megabytes).

	Default value: 8192.
Limit CPU usage by scan tasks (%)	The checkbox 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 number specified in **Upper limit (%)**. This check box is cleared by default.

Setting a limit in the Administration Console

In the Administration Console, you can enable and disable the CPU utilization limit and configure the memory usage limit for scan tasks in the policy properties (**General settings** → **Application settings**, **Performance** section).

Under **Performance**, clicking the **Configure** button opens **the CPU and memory usage** window, in which you can configure limits (see the table below).

Settings

Setting	Description
Limit CPU usage for scan tasks (%)	The checkbox 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. 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.

Setting a limit on the command line

In the command line, you can configure CPU utilization limits for *ODS*, *ContainerScan*, and *InventoryScan* tasks using the `UseOnDemandCPULimit` and `OnDemandCPULimit` settings in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

`UseOnDemandCPULimit` accepts the following values:

- `Yes`: enable the CPU usage limit for *ODS*, *ContainerScan*, and *InventoryScan* tasks.
- `No`: disable the CPU usage limit for tasks.

The `OnDemandCPULimit` option sets the maximum utilization level for all processor cores (as a percentage) when running *ODS*, *ContainerScan*, and *InventoryScan* tasks. The option accepts values between 10 and 100. Default value 100.

In the command line, you can configure memory usage limits for *ODS*, *ContainerScan*, and *InventoryScan* tasks using the `ScanMemoryLimit` setting in the kesl.ini configuration file. Default value: 8192.

Limiting the use of resident memory by the application

You can configure a limit on the application's use of resident memory. By default, the limit is set automatically.

Setting a limit in the Web Console

In the Web Console, you can enable or disable the resident memory usage limit in the policy properties (**Application settings** → **General settings** → **Application settings**, **Advanced application settings** section).

In the **Advanced application settings** section, the **Configure memory usage** link opens a window where you can configure the resident memory usage limit (see the table below).

Settings

Setting	Description
Resident memory usage by the application	In the drop-down list, you can select how to limit resident memory usage: • **Unlimited**. When this item is selected, resident memory usage is not limited. • **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. • **Limit automatically (recommended)**. When this item is selected, resident memory usage is limited automatically (default value).
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.

Setting a limit in the Administration Console

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).

Settings

Setting	Description
Application memory	In the drop-down list, you can select how to limit resident memory usage: • **Unlimited**. When this item is selected, resident memory usage is not limited.

usage	• **Limit 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.

Setting a limit on the command line

In the command line, you can configure the resident memory usage limit using the `MaxMemory` setting in the kesl.ini configuration file.

The `MaxMemory` setting can take the following values:

- `off` – the resident set size is not limited.
- < `value` >% – a value between 1 and 100, expressing a percentage of memory.
- < `value` >`MB` – a value in megabytes.
- `lowest/`< `value` >%/< `value` >`MB` – the smaller value between the value as a percentage and the value in megabytes.
- `highest/`< `value` >%/< `value` >`MB` – the larger value between the value as a percentage and the value in megabytes.
- `auto` – up to 50% of available memory, but not less than 2 GB and not more than 16 GB.

Default value: `auto`.

Limiting the number of Custom Scan tasks

You can set a limit on the number of custom scan tasks that a non-privileged user can simultaneously run on a device. There is no limit on the number of tasks that a user with root privileges can run.

You can enable or disable the limit on the number of concurrent custom scan tasks on the command line using the `LimitNumberOfScanFileTasks` option in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

`LimitNumberOfScanFileTasks` accepts values between 0 and 4294967295. Default value: 0.

If 0 is specified, a non-privileged user cannot start custom scan tasks.

If you installed the graphical user interface package when installing the application, the `LimitNumberOfScanFileTasks` settings has the default value `5`.

Configuring the sending of information to Kaspersky Security Center Backup

In Kaspersky Security Center, you can enable or disable forwarding of information about unprocessed files and connected devices to the Kaspersky Security Center storage.

Information about unprocessed files is displayed in the list of active threats in the Web Console (**Operations** → **Storages** → **Active threats**) and in the Administration Console (**Advanced** → **Storages** → **Active threats**).

Information about devices installed on or connected to a client device is displayed in the list of hardware in the Web Console (**Operations** → **Storages** → **Hardware**) and in the Administration Console (**Advanced** → **Storages** → **Hardware**). Information is forwarded if Device Control is enabled.

Enabling or disabling forwarding of information in the Web Console

In the Web Console, you can enable or disable sending information in the policy properties (**Application settings** → **General settings** → **Storage settings**).

Settings for forwarding of information to the Kaspersky Security Center storage

Setting	Description
Informing about unprocessed files enabled / disabled	This toggle switch enables or disables sending notifications about the files, that cannot be processed during the scan, to the Administration Server. The check toggle button is switched on by default.
Informing about installed devices enabled / disabled	This toggle sitch enables or disables forwarding of information about devices installed on a client device or connected to it, to the Administration Server. This toggle switch is turned on by default.

Enabling and disabling forwarding of information in the Administration Console

In the Administration Console, you can enable or disable sending information in the policy properties (**General settings** → **Storage settings**).

Settings for forwarding of information to the Kaspersky Security Center storage

Setting	Description
Notify about unprocessed	This check box enables or disables sending notifications about the files, which cannot be processed during the scan, to the Administration Server.

files	The check box is selected by default.
Notify about installed devices	This check box enables or disables forwarding of information about devices installed on a client device or connected to it, to the Administration Server. The check box is selected by default.

Configuring permissions for task management

You can define the following user permissions in Kaspersky Security Center:

- Viewing tasks created in Kaspersky Endpoint Security
- Viewing tasks created in Kaspersky Security Center on client devices

Configuring in the Web Console

In the Web Console, you can set the permission to view tasks in the policy properties (**Application settings** → **Local Tasks** → **Task management**).

Task management settings

Setting	Description
Allow users to view and manage 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. This check box is cleared by default.
Allow users to view and manage tasks created through KSC	The check box allows or prohibits the users from viewing tasks created in Kaspersky Security Center Web Console and managing these tasks on managed client devices. This check box is cleared by default.

Configuring in the Administration Console

In the Administration Console, you can set the permission to view tasks in the policy properties (**Local Tasks** → **Task management**).

Task management settings

Setting	Description
Allow users to view and manage 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. This check box is cleared by default.
Allow users to view and manage tasks created through KSC	The check box allows or prohibits the users from viewing the tasks created in Kaspersky Security Center and managing these tasks on the managed client devices. This check box is cleared by 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.

If the file is successfully disinfected, the status of the backup copy changes to *Disinfected*. Sometimes it is not possible to maintain the integrity of files during disinfection. If you partially or completely lose access to important information in a disinfected file after disinfection, you can attempt to restore the file from the disinfected copy to the file's original directory.

We recommend restoring files from backup copies only if these have a status of *Disinfected*. Restoring infected objects may lead to a device infection.

Backup file copies may contain personal data. Root privileges are required to access Backup objects.

You can configure the following Backup settings:

- Storage time for objects in Backup. Objects are kept for 90 days by default.
- Maximum Backup size. Backup has an unlimited size by default.
- Path to Backup. By default, the Backup storage is located in the /var/opt/kaspersky/kesl/common/objects-backup/ directory.

When the specified retention period expires, or when the maximum Backup size is reached, the application automatically deletes backup copies regardless of their status.

You can delete the backup copy of a restored or unrestored file manually.

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** → **Storages** → **Backup**) and in the Web Console (**Operations** → **Storages** → **Backup**). You can view the properties of backup copies on protected devices, run malware scans in Backup, and delete files. Kaspersky Security Center does not copy files from Backup to the Administration Server; all files are stored in the Backup storages on protected devices. File restore takes place on the protected device.

Configuring Backup settings in the Web Console

In the Web Console, you can configure Backup settings in the policy properties (**Application settings** → **General settings** → **Storage settings**).

Backup settings

Setting	Description
Notification about files in Backup is enabled/disabled	This toggle switch enables or disables sending of notifications about files in the Backup storage to the Administration Server. The check toggle button is switched on by default.
Store objects no longer than	The entry field to specify the period for storing objects in the Backup

(days)	storage. Available values: 0–3653. Default value: 90. If 0 is specified, the period for storing objects in the Backup storage is unlimited.
Limit the size of Backup to (MB)	The entry field to specify the maximum size of the Backup storage (MB). Available values: 0–999999. Default value: 0 (unlimited).

Configuring Backup settings in the Administration Console

In the Administration Console, you can configure Backup settings in the policy properties (**General settings** → **Storage settings**).

Backup settings

Setting	Description
Inform about files in Backup	This check box enables or disables sending of notifications about the files in the Backup storage to the Administration Server. The check box is selected by default.
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. Available values: 0–3653. Default value: 90. If 0 is specified, the period for storing objects in the Backup storage is unlimited.
Limit the size of Backup to (MB)	This check box enables or disables the maximum Backup storage size (in megabytes). Available values: 0–999999. Default value: 0 (unlimited).

Configuring Backup settings in the command line

You can configure Backup in the command line via the *Backup* predefined task.

The Backup management task is started by default. You cannot start or stop it manually.

You can configure Backup by editing the settings for the Backup management predefined task.

Backup management task settings

Setting	Description	Value
`DaysToLive`	Time period for storing objects in the Backup storage (in days). To remove the object retention limit, set 0.	0: unlimited retention. Default value: 90.
`BackupSizeLimit`	Maximum Backup size in MB. When the maximum Backup storage size is reached, the application deletes the oldest objects. To remove the Backup size limit, set 0.	0 – 999999 0: unlimited size. Default value: 0.

`BackupFolder`	Path to the Backup directory. You can specify a custom Backup storage directory that is different from the default directory. You can use directories on any device as the Backup storage. It is not recommended to assign directories that are located on remote devices, such as those mounted via the Samba and NFS protocols. Kaspersky Endpoint Security starts moving the objects to the specified directory after you change the settings and restart the application. 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.

Working with Backup objects in the command line

You can use the Backup management commands in the command line for the following actions on Backup objects:

- View Backup object details.
- Delete some or all objects from Backup.
- Restore objects from Backup.

Restoring infected objects may lead to a device infection.

Viewing Backup object details

To view the details of the objects in Backup, run:

```
kesl-control -B --query ["<filter conditions>"] [-n <number>] [--json]
```

where:

- `<filter conditions>`: one or several logical expressions in the format `<field> <comparison operator> '<value>'`, combined with the help of the logical operator `and` to limit the results. If you do not specify any filter conditions, the application will display the details of all objects in Backup.
- `<number>`: the number of the most recent objects to display. If you do not specify the `-n` switch, the last 30 objects will be displayed. Specify 0 to show all objects.
- `--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.

Restoring objects from Backup

To restore an object under its original name to its original location, execute the following command:

```
kesl-control --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 a specified directory, execute the following command:

```
kesl-control --restore <object ID> --file <file name and path>
```

where `--file <file name and path>` 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.

Deleting objects from Backup

To remove selected objects from Backup, run:

```
kesl-control --mass-remove --query "<filter conditions>"
```

`where <filter conditions>` is one or several logical expressions in the format `<field> <comparison operator> '<value>'`, combined with the help of the logical operator `and` to limit the results.

Examples:
To remove an object with ID=15:

```
kesl-control -B --mass-remove --query "ObjectId == '15'"
```

To 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
```

Integration with Detection and Response solutions

Detection and Response solutions by Kaspersky are security systems designed to detect advanced threats and attack signs at various levels of the organization's infrastructure. Detection and Response solutions provide information about the detected threat and let you manage your response to detections.

Kaspersky Endpoint Security interoperates with the following Kaspersky Detection and Response solutions:

- Kaspersky Anti Targeted Attack Platform (Kaspersky Endpoint Detection and Response component). Integration with Kaspersky Endpoint Detection and Response (KATA) is facilitated by a Kaspersky Endpoint Security component: Endpoint Detection and Response (KATA) (EDR (KATA)).
- 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).

If Kaspersky Endpoint Security is integrated with Kaspersky Managed Detection and Response and Kaspersky Anti Targeted Attack Platform, a large number of events can be written to the systemd log. If you want to disable the logging of audit events to the systemd log, disable the systemd-journald-audit socket and restart the operating system.

To disable the systemd-journald-audit socket, run the following commands:

```
systemctl stop systemd-journald-audit.socket

systemctl disable systemd-journald-audit.socket

systemctl mask systemd-journald-audit.socket
```

By default, on the SintezM-Client operating system, the auditd service configuration is protected from modification, 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.

About response actions for commands of Detection and Response solutions

Kaspersky Endpoint Security can perform response actions aimed at providing security functions:

- When interacting with Kaspersky Endpoint Detection and Response (KATA), a component of the Kaspersky Anti Targeted Attack Platform solution.
- When interacting with Kaspersky Endpoint Detection and Response Optimum.

The response action settings of Kaspersky Anti Targeted Attack Platform and Kaspersky Endpoint Detection and Response Optimum are different.

Kaspersky Endpoint Security can perform the following response actions:

- Get files from devices.

  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 program.

- Delete files from devices.

  This action is performed using the *Delete file* task.

- Remotely run processes on devices.

  This action is performed using the *Run process* task.

  For example, you can remotely run a utility that creates a device configuration file, and then fetch it with *Get file*.

- Remotely terminate processes on devices.

  The action is performed using the *Terminate process* task.

  For example, you can remotely terminate an Internet speed test utility that was launched using the "Run process" task.

- Detect *Indicators of Compromise* on devices and perform threat response actions.

  This action is performed using the *IOC Scan* task.

  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 the hash of files larger than 200 MB.

- Enable or disable network isolation of the device.

  When Kaspersky Endpoint Security interacts with Kaspersky Endpoint Detection and Response Optimum, you can:

  - Enable or disable network isolation in the Web Console or Kaspersky Security Center Cloud Console.
  - Disable network isolation in the command line.
  - Configure automatic disabling of network isolation in the Web Console or Kaspersky Security Center Cloud Console.

  When Kaspersky Endpoint Security interacts with Kaspersky Endpoint Detection and Response (KATA), you can:

  - Disable network isolation in the command line.
  - Enable or disable network isolation in the Kaspersky Endpoint Detection and Response (KATA) solution.

    To read more, check out the Kaspersky Anti Targeted Attack Platform Help.

Network isolation limitations

When you use network isolation, we strongly recommended that you familiarize yourself with the limitations described below.

For network isolation to work, Kaspersky Endpoint Security must be running. If Kaspersky Endpoint Security malfunctions (and the application is not running), traffic blocking is not guaranteed when network isolation is enabled by Kaspersky Anti Targeted Attack Platform or Kaspersky Endpoint Detection and Response Optimum.

Transit traffic with network isolation enabled is supported with limitations and may be filtered.

DHCP and DNS are not automatically added to network isolation exceptions, so if the network address of a resource is changed during network isolation, Kaspersky Endpoint Security will not be able to access 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 also not automatically added 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 KATA server.

Adding a process to network isolation and excluding a process from network isolation by name is not supported.

If Kaspersky Endpoint Security is used in standard mode, we recommend doing the following when using network isolation:

- 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, configure the settings of the required proxy server and add it to the 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.

Kaspersky Endpoint Detection and Response (KATA) Integration

Kaspersky Endpoint Detection and Response (KATA) is a component of the Kaspersky Anti Targeted Attack Platform solution. Integration with the Kaspersky Endpoint Detection and Response (KATA) component is facilitated by a Kaspersky Endpoint Security component: Endpoint Detection and Response (KATA) (EDR (KATA)).

Kaspersky Endpoint Security is compatible with the Kaspersky Anti Targeted Attack Platform solution, which is designed to protect the IT infrastructure of organizations and promptly detect threats, such as zero-day attacks, targeted attacks, and advanced persistent threats (APT). To read more, check out the Kaspersky Anti Targeted Attack Platform Help.

This feature is not supported in the KESL container.

When interacting with Kaspersky Endpoint Detection and Response (KATA), Kaspersky Endpoint Security can:

- Send data about events on devices (telemetry) to the Kaspersky Anti Targeted Attack Platform server with the Central Node component ("KATA server"). Kaspersky Endpoint Security sends monitoring data on processes, open network connections, and modified files to the KATA server, as well as data on threats detected by the application and data on the results of processing these threats.
- Execute response actions to ensure security when receiving commands from Kaspersky Anti Targeted Attack Platform.

For integration with Kaspersky Endpoint Detection and Response (KATA), the Behavior Detection component must be enabled.

Integration of the Kaspersky Endpoint Security application with Kaspersky Endpoint Security and EDR (KATA) is possible only with Behavior Detection enabled. Otherwise, the required telemetry data cannot be transmitted.

Kaspersky Endpoint Detection and Response (KATA) can additionally use data received from the following components:

- File Threat Protection.
- Network Threat Protection.
- Web Threat Protection.

When integrated with Kaspersky Endpoint Detection and Response (KATA), devices with Kaspersky Endpoint Security establish secure connections to the KATA server via the HTTPS protocol. To ensure a secure connection, the following certificates issued by the KATA server are used:

- KATA server certificate. The connection is encrypted using the server's TLS certificate. You can elevate the security of the connection by verifying the server certificate on the Kaspersky Endpoint Security side. To do this, add the integration server certificate before enabling the Kaspersky Endpoint Detection and Response (KATA) Integration.
- Client certificate. This certificate is used for additional protection of the connection using two-way authentication (scanning devices with Kaspersky Endpoint Security KATA server). The same client certificate can be used by multiple devices. By default, the KATA server does not check client certificates, but two-way authentication can be enabled on the Kaspersky Anti Targeted Attack Platform side. In this case, you need to enable two-way authentication in the Kaspersky Endpoint Detection and Response (KATA) Integration settings and add the client certificate (cryptocontainer with certificate and private key).

Certificates for securing the connection to the KATA server are provided by the Kaspersky Anti Targeted Attack Platform administrator.

A proxy server is used to connect to the KATA server if use of a proxy server is configured in the general application settings of Kaspersky Endpoint Security.

By default, the Kaspersky Endpoint Detection and Response (KATA) Integration is disabled. You can enable or disable the integration, and configure the following integration settings via the command line, Web Console, and Administration Console:

- Configure general KATA server connection settings.
- Add or remove KATA server certificates.
- Configure two-way authentication when connecting to KATA servers and add client certificates.
- Configure event forwarding.
- Enable or disable sending telemetry.

If integration between Kaspersky Endpoint Security and Kaspersky Managed Detection and Response is enabled, process exclusions are not applied when sending telemetry.

Managing Kaspersky Endpoint Detection and Response (KATA) Integration settings in Kaspersky Security Center Cloud Console is not supported.

Configuring the Kaspersky Endpoint Detection and Response (KATA) integration in the Web Console

In the Web Console, you can enable or disable the integration of Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response (KATA) and configure integration settings in the policy properties (**Application settings** → **Detection and Response** → **Endpoint Detection and Response (KATA)**).

Managing Kaspersky Endpoint Detection and Response (KATA) Integration settings in Kaspersky Security Center Cloud Console is not supported.

Kaspersky Endpoint Detection and Response (KATA) integration settings

Setting	Description
Endpoint Detection and Response (KATA) enabled/disabled	Enables or disables the integration of the Kaspersky Endpoint Security application with Kaspersky Endpoint Detection and Response (KATA). The integration server is disabled by default.
Server connection settings	Clicking the **Configure** link 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.
KATA servers	The table contains a list of KATA servers to which connection is configured. The **Add** button opens a window where you can configure the connection to the KATA server. You can use the buttons above the table to edit and remove previously configured connection settings.
Maximum delay when sending events (sec)	The maximum delay in sending events to the KATA server in seconds. The default value is `30`.
Enable event throttling	Enables or disables regulating the number of events sent to the KATA server.
Maximum number of events per hour	Maximum number of events per hour The default value is `3000`.
Event throttle threshold (percentage)	Event throttle threshold (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). The default value is `15`.

Server connection settings window

In this window, you can configure general settings for connecting to KATA servers, add a server certificate, and configure two-way authentication when connecting to KATA servers.

Setting	Description
Send a synchronization request to the KATA server every (minutes)	Frequency of sending synchronization requests to the KATA server in minutes. The default value is `5`.
Maximum time to wait for the server connection (sec)	Maximum time to wait for a connection to the KATA server in seconds. The default value is `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. The default value is `10`.
Allow sending telemetry	Enables or disables sending data about events on devices (telemetry) to the KATA server. Sending telemetry is enabled by default.
Server certificate	After adding the server certificate, information about the certificate is displayed: • certificate serial number • certificate subject • certificate issuer • certificate start date • certificate expiration date
Select	Opens a standard file selection window where you can specify the path to the KATA server certificate. 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.
Remove	Deletes the server certificate added previously. The button is displayed only if a server certificate has been added.
Additional connection protection	The settings section lets you enable or disable two-way authentication when connecting to the KATA server and add a client certificate.
Use two-factor authentication	Enables or disables the use of two-way authentication to further secure the connection to the KATA server. Two-way authentication must be enabled on the KATA server side. To use two-factor authentication, you need to add a client certificate.
Add client certificate	Opens a standard file selection window where you can specify the path to the cryptocontainer (PFX archive) with the client certificate and private key. The button is available if the **Use two-factor authentication** checkbox is selected.
Edit	Allows you to specify the password for the cryptocontainer with the client certificate. The **Cryptocontainer password** field cannot be edited. By default, the password is empty.

	To specify a password, click **Edit**. In the window that opens, enter the password and click **OK**. Clicking the **Show** button in the window displays the password in clear text in the password entry window. It is recommended to make sure that the password complexity and anti-bruteforce mechanisms ensure that the password cannot be guessed within 6 months. The button is available if the **Use two-factor authentication** checkbox is selected.

Settings window to connect to the KATA server

In this window you can specify the connection settings to the KATA server.

KATA 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 KATA server is not interrupted if the application fails when network isolation is enabled for the device, it is recommended to specify the server's IP address. Default value: `127.0.0.1`.
Port	Port to connect to the KATA server. The default value is `443`.

Configuring the Kaspersky Endpoint Detection and Response (KATA) integration in the Administration Console

In the Administration Console, you can enable, disable, or configure the integration between Kaspersky Endpoint Security and Kaspersky Endpoint Detection and Response (KATA) in the policy properties (**Detection and Response → Endpoint Detection and Response (KATA)**).

Kaspersky Endpoint Detection and Response (KATA) integration settings

Setting	Description
Integration with Endpoint Detection and Response (KATA).	Enables or disables the integration of the Kaspersky Endpoint Security application with Kaspersky Endpoint Detection and Response (KATA). The integration server is disabled by default.
KATA servers	The **Configure** button opens the **KATA servers** window. In this window, you can configure a connection to KATA servers and view the list of servers to which a connection is 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 data to KATA servers.

KATA servers window

The table in the window displays the list of settings for connecting to 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

Settings window to connect to the KATA server

In this window you can specify the connection settings to the KATA server.

KATA 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 KATA server is not interrupted if the application fails when network isolation is enabled for the device, it is recommended to specify the server's IP address. Default value: `127.0.0.1`.
Port	Port to connect to the KATA server. The default value is `443`.

Server connection settings window

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 (minutes)	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. The default value is `10`.
Maximum time to wait	Maximum time to wait for a response from the KATA server in seconds.

for a response from the server (sec)	The default value is `10`.
Allow sending telemetry	Enables or disables sending data about events on devices (telemetry) to the KATA server. Sending telemetry is enabled by default.
Use two-factor authentication	Enables or disables the use of two-way authentication to further secure the connection to the KATA server. To use two-factor authentication, you need to add a client certificate. Two-way authentication must be enabled on the KATA server side.
Add (client certificate)	Opens the window for adding a client certificate for additional security of the connection with the KATA 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 KATA server side and select the **Use two-factor authentication** checkbox in this window.
Remove (client certificate)	Removes the client certificate. The button is displayed if a client certificate has been added.
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.

Adding a server certificate window

In this window, you can add a KATA 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 KATA server.

If you want to configure additional protection for the connection, enable verification of the client certificates on the KATA server side and select the **Use two-factor authentication** checkbox in the 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. If the archive is password-protected, enter the password in the **Cryptocontainer password** field.

Data transfer settings window

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. The default value is `30`.
Enable event throttling	Enables or disables regulating the number of events sent to the KATA server.
Maximum number of events per hour	Maximum number of events per hour The default value is `3000`.
Event throttle threshold (percentage)	Event throttle threshold (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). The default value is `15`.

Configuring the Kaspersky Endpoint Detection and Response (KATA) integration on the command line

You can manage the integration between Kaspersky Endpoint Security and Kaspersky Endpoint Detection and Response (KATA) via the Kaspersky Endpoint Detection and Response (KATA) Integration (*KATAEDR*) predefined task in the command line.

The Kaspersky Endpoint Detection and Response (KATA) Integration does not run by default. You can start and stop this task manually.

You can configure Kaspersky Endpoint Detection and Response (KATA) Integration settings by editing the settings of the predefined task.

Using the commands for managing the Kaspersky Endpoint Detection and Response (KATA) integration settings, you can manage certificates that are used for connecting to KATA servers.

Kaspersky Endpoint Detection and Response (KATA) Integration task settings

The table describes all available settings and the default values of all the settings that you can specify for the Kaspersky Endpoint Detection and Response (KATA) Integration task.

Kaspersky Endpoint Detection and Response (KATA) Integration task settings

Setting	Description	Value
`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 KATA server is not interrupted if the application fails when network isolation is enabled for the device, it is recommended to specify the server's IP address.	Default value: `127.0.0.1`.
`Port`	Port to connect to the KATA server.	The default value is `443`.
`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 (KATA) Integration task and add the client certificate before starting the task.	`Yes` – use two-factor authentication to further secure the connection to the KATA server. `No` (default value) — do not use two-factor authentication.
`SynchronizationPeriod`	Frequency of sending synchronization requests to the KATA server in minutes.	The default value is `5`.
`ConnectionTimeout`	Maximum time to wait for a connection to the KATA server in seconds.	The default value is `10`.
`RequestTimeout`	Maximum time to wait for a response from the KATA server in seconds.	The default value is `10`.
`MaximumDataTransferTime`	The maximum delay in sending events to the KATA server in seconds.	The default value is `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.
`MaximumNumberOfEventsInHour`	Maximum number of events per hour	The default value is `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).	The default value is `15`.

`EnableTelemetry`	Enable and disable sending event data (telemetry) to the KATA server.	`Yes` (default value) – send telemetry to the KATA server. `No` – do not send telemetry.

Managing certificates for connecting to KATA servers

Root privileges are required to manage certificates.

You can manage certificates used to connect to KATA servers using commands. What you can do 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 [-R] --add-kataedr-server-certificate <file name and path>
```

where <`file name and path`> are the name and path to the file containing the server certificate.

To add or change a client certificate:

1. Execute the command:

   ```
   kesl-control [-R] --add-kataedr-client-certificate <file name and path>
   ```

   where <`file name and path`> is the name and 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 KATA server if client certificate verification is enabled in KATA server settings and in the Kaspersky Endpoint Detection and Response (KATA) Integration task settings the `UseClientPinnedCertificate` setting has the value `yes`.

To display certificate information, run the following command:

- for the server certificate:

```
kesl-control [-R] --query-kataedr-server-certificate
```

- for the client certificate:

  ```
  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
```

If certificate usage is configured in the settings of Kaspersky Endpoint Detection and Response (KATA) Integration task and the task is running, deletion of this certificate ends with an error.

Kaspersky Endpoint Detection and Response Optimum Integration

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 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 response actions in a timely manner.

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).

Kaspersky Endpoint Security 12.1 for Linux is compatible with Kaspersky Endpoint Detection and Response Optimum version 3.0.

Versions of Kaspersky Endpoint Security for Linux earlier than 12.1 do not include the EDR Optimum component.

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 response actions to ensure security when receiving commands from Kaspersky Security Center.

Integration with Kaspersky Endpoint Detection and Response Optimum involves the following steps:

1. **Enabling required components of Kaspersky Endpoint Security**

   Make sure that the following components of Kaspersky Endpoint Security are enabled and running:

   - File Threat Protection.
   - Web Threat Protection.
   - Behavior Detection.

2. **Enabling threat analysis tools**

   Make sure that Kaspersky Security Network is enabled 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.

3. **Activating the EDR Optimum component**

   Make sure one of the following conditions is satisfied:

   - You are using Kaspersky Endpoint Security under a license that includes the Kaspersky Endpoint Detection and Response Optimum functionality.
   - You have purchased a separate license for using the Kaspersky Endpoint Detection and Response Optimum functionality and also added the EDR Optimum license key to the application.

4. **Enabling the Kaspersky Endpoint Detection and Response Optimum Integration**

   By default, the integration of Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Optimum is disabled. You can enable, disable, or configure the integration:

   - Using the Web Console or Kaspersky Security Center Cloud Console.
   - Using the command line.

Managing the EDR Optimum component using Kaspersky Security Center Administration Console is not supported.

You can check the status of the EDR Optimum component:

- Using the *Application component status report* in Web Console or Kaspersky Security Center Cloud Console.

  The **Endpoint Detection and Response Optimum** component has been added to the list of Kaspersky Endpoint Security components. For detailed information about reports, please refer to the Kaspersky Security Center Help.

- In the device properties in the Web Console or Kaspersky Security Center Cloud Console.

- Using the command line.

5. **Enabling data transfer to the Administration Server**

   To use all functionality of Kaspersky Endpoint Detection and Response Optimum, you must enable the following settings:

   - **Notification about files in Backup is enabled/disabled**.

     You can enable this setting in the policy properties under **Application settings** → **General settings** → **Storage settings**.

     By enabling this setting, you allow information about files that Kaspersky Endpoint Security has moved to Backup on the device to be sent to Kaspersky Security Center.

   - **Show EDR alerts**.

     You can enable this setting in the main window of Kaspersky Security Center Web Console under **Settings** → **Interface settings**.

     By enabling this setting, you allow the list of alerts to be displayed.

     The **Show EDR alerts** setting not available in a Web Console version earlier than 15.1.

Enabling or disabling Kaspersky Endpoint Detection and Response Optimum integration

You can enable or disable the Kaspersky Endpoint Detection and Response Optimum Integration:

- Using the Web Console or Kaspersky Security Center Cloud Console.
- Using the command line.

The Administration Console does not support managing the settings for integrating Kaspersky Endpoint Detection and Response Optimum.

Enabling or disabling Kaspersky Endpoint Detection and Response Optimum integration in the Web Console

In the Web Console or Kaspersky Security Center Cloud Console, you can enable or disable the integration of Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Optimum and configure the integration settings:

- In the policy properties (**Application settings** → **Detection and Response** → **Endpoint Detection and Response Optimum**)
- In the device properties (**Assets (Devices)** → **Managed devices** → <device name> link → **Applications** → <Kaspersky Endpoint Security 12.1 for Linux application name> link → **Application settings** → **Detection and Response** → **Endpoint Detection and Response Optimum**)

  Enabling or disabling the integration of Kaspersky Endpoint Security with Kaspersky Endpoint Detection and Response Optimum in the device properties is not available if the policy is being applied to the device.

  Kaspersky Endpoint Detection and Response Optimum integration settings

Setting	Description
Endpoint Detection and Response Optimum is enabled/disabled	Enables or disables the integration of the Kaspersky Endpoint Security application with Kaspersky Endpoint Detection and Response Optimum. The integration server is disabled by default.
Network isolation	The **Configure device unblocking** link opens the **Configure device unblocking** window, where you can configure the duration of device blocking.
Exclusions	The **Exclusions** link opens the **Exclusions** window in which you can configure network isolation exclusions.

Enabling or disabling Kaspersky Endpoint Detection and Response Optimum integration on the command line

On the command line, you can enable or disable the integration with Kaspersky Endpoint Detection and Response Optimum using the `UseEdrOptimum` setting in the general application settings.

You can edit the setting using command line options or a configuration file that contains all general application settings.

To enable the Kaspersky Endpoint Detection and Response Optimum integration using command line options, run the following command:

```
kesl-control --set-app-settings UseEdrOptimum=Yes
```

To disable the Kaspersky Endpoint Detection and Response Optimum integration using command line options, run the following command:

```
kesl-control --set-app-settings UseEdrOptimum=No
```

Viewing the Kaspersky Endpoint Detection and Response Optimum integration status

Viewing the integration status in the Web Console or Kaspersky Security Center Cloud Console

You can view the status of integration with Kaspersky Endpoint Detection and Response Optimum in the Web Console or Kaspersky Security Center Cloud Console by selecting **Assets (Devices)** → **Managed devices** → <device name> link → **Applications** → <Kaspersky Endpoint Security 12.1 for Linux application name> link → **General** → **Components**.

Viewing the integration status on the command line

You can view the status of integration with Kaspersky Endpoint Detection and Response Optimum using the command line by running the `kesl-control --app-info` command.

Integration statuses

One of the following statuses is displayed for the EDR Optimum component:

- *Running*.

  This status is displayed when the following conditions are simultaneously satisfied:

  - A license key required by EDR Optimum is added.
  - The current date is earlier than the license expiration date.
  - One or more Kaspersky Endpoint Security components that EDR Optimum requires are enabled.
  - Kaspersky Endpoint Detection and Response Optimum Integration is enabled on the device.

- *Stopped*.

  This status is displayed in the following cases:

  - Kaspersky Endpoint Detection and Response Optimum Integration is disabled.
  - The Kaspersky Endpoint Security application is not stopped.

- *Not supported by license*.

  This status is displayed in the following cases:

  - The current date is later than the license expiration date.
  - The current license does not include the EDR Optimum functionality.

- *Malfunction*.

  This status is displayed when the following conditions are simultaneously satisfied:

- The current date is earlier than the license expiration date.
- One or more Kaspersky Endpoint Security components that EDR Optimum requires has run into an error.

Viewing information about a detected threat and response actions

To view all information about a detected threat and perform appropriate threat response actions, you can use the alert details window, which contains:

- Threat development chain graph
- Recommendations for responding to the threat with the UI for performing the chosen action
- General information about the threat detection (for example, the detection mode)
- Information about the protected device
- Information about the detected object
- History of files appearing on the device
- Information about the threat response actions performed by the application

For more details about managing alert details, refer to the Kaspersky Endpoint Detection and Response Optimum Help.

IOC Scan results are stored for 30 days. After this time expires, Kaspersky Endpoint Security automatically deletes old entries.

Searching for indicators of compromise

You can search for indicators of compromise on the device and perform threat response actions using the *IOC Scan* task.

To search for indicators of compromise, Kaspersky Endpoint Security uses IOC files prepared by the user. IOC files must comply with the IOC file requirements.

You can create and run an *IOC Scan* task as well as change its settings in the Web Console or Kaspersky Security Center Cloud Console:

- In the **Assets (Devices)** → **Tasks** section
- In the **Assets (Devices)** → **Managed devices** → <device name> link → **Tasks** section
- In the alert details window

You cannot create, run, or configure the *IOC Scan* task on the command line. *IOC Scan* tasks created in the Web Console or Kaspersky Security Center Cloud Console cannot be viewed using the `kesl-control --get-task-list` command in the command line.

The Wake-on-LAN functionality is not available for this task in schedule settings. For the task to run, make sure the device is powered on.

IOC Scan task settings

Setting	Description
Redefine IOC files	This button opens the **Redefine IOC files** panel. Clicking the **Add IOC files** button located in the **Redefine IOC files** panel opens a window where you can select and download the IOC files on the device that are necessary to search for indicators of compromise. After uploading the IOC files, you can view a list of indicators from the IOC files.
Export IOC collection	Clicking this button downloads IOC files to the device.
Apply response actions when an IOC is detected	This check box enables or disables the application of response actions when indicators of compromise are detected. If the check box is selected, then when indicators of compromise are detected, the application performs the actions you selected: • **Isolate device from the network**. If this check box is selected, then when indicators of compromise are detected, the application isolates the device from the network to prevent the spread of the threat. You can configure the isolation duration. • **Start critical areas scan**. If this check box is selected, then when indicators of compromise are detected, the application starts the *Critical Areas Scan* task. By default, Kaspersky Endpoint Security scans the kernel memory, running processes, and boot sectors. If the check box is cleared, the application does not perform any response actions when indicators of compromise are detected. Information about detected indicators of compromise is displayed in the window with alert details and in the task properties.
Scan scopes	The file scan areas are displayed: the critical areas of the system disks and the path from the IOC.

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.

You can see the result of the *IOC Scan* in the **Assets (Devices)** section → **Tasks** → <task name> → **Application settings** → **IOC Scan results**.

The table in the **IOC Scan results** section contains a list of devices on which the *IOC Scan* task has been run, as well as the results of the task. In the **Device** drop-down list, you can select the task results for all managed devices in the administration group or for a specific device.

The table contains the following columns:

- **Status**.

  Status of indicator of compromise detection, displayed as an icon.

- **Host**.

Name of the device on which the *IOC Scan* task was run.

- **Time**.

  Date and time when the *IOC Scan* task was performed.

- **Results**.

  Information about the result of the *IOC Scan* task. A completed task can have one of the following statuses:

  - *IOCs detected*

    This status is displayed as a link; clicking the link opens a window with the alert details.

  - *No IOCs detected*

You can also view the result of the task in the **Assets (Devices)** → **Tasks** → <task name> section, on the **Results** tab in the **Description** column.

IOC Scan results are stored for 30 days. After this time expires, Kaspersky Endpoint Security automatically deletes old entries.

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 and XML extensions. These files use open standard for IOC description – OpenIOC versions 1.0 and 1.1.
- 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. Duplicate IDs may affect the correctness of task results.
- The size of an IOC file may not exceed 2 MB. Larger files cause IOC Scan tasks to fail. The total size of all added files in an IOC collection may not exceed 10 MB. If the total size of all files is greater than 10 MB, you must split the IOC collection and create multiple *IOC Scan* tasks.
- 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 IOC_TERMS.XLSX

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.

Enabling or disabling device network isolation

You can enable network isolation for a device in the following ways:

- Using the *IOC Scan* task.

  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 (IOCs).

- In the alert details window

- In the device properties in the Web Console or Kaspersky Security Center Cloud Console.

> Enabling network isolation is available only if integration with Kaspersky Endpoint Detection and Response Optimum is enabled and the EDR Optimum component has the In progress status.

You can disable network isolation for a device in the following ways:

- Manually in the device properties in the Web Console or Kaspersky Security Center Cloud Console.
- Manually on the command line.
- In the alert details window.
- By configuring automatic disabling in the device properties or in the policy properties.

> Disabling network isolation in the device properties and in the command line is available regardless of whether integration with Kaspersky Endpoint Detection and Response Optimum is enabled and the EDR Optimum component is enabled, or whether a policy is applied to the device.

You can configure exclusions for network connections that do not need to be isolated when network isolation is enabled.

You can check the network isolation status on the command line.

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.

An isolated EDR Optimum device automatically gets 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.

Manually enabling or disabling the network isolation of the device in the Web Console

To enable or disable network isolation for a device:

1. In the main window of the Web Console or Kaspersky Security Center Cloud 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 the name of the **Kaspersky Endpoint Security 12.1 for Linux** application.

   The application properties window opens.

6. Go to the **Application settings** tab.

7. Go to **Detection and Response** → **Endpoint Detection and Response Optimum** section.

8. Under **Network isolation**, do one of the following:

   - to enable network isolation of the device, click the **Isolate device from the network** button
   - to disable network isolation of the device, click the **Unblock an isolated device** button

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.

Configuring the automatic disabling of network isolation

You can configure network isolation to be disabled automatically after a specified period of time:

- In the device properties.

  Configuring automatic disabling of network isolation in the properties of a device is not available if the policy is applied to the device.

- In the policy properties.

  The settings for automatically disabling network isolation specified in policy properties apply only to devices that were isolated as a result of detected Indicators of Compromise (IOC) during an *IOC Scan* task.

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 or Kaspersky Security Center Cloud 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 the name of the **Kaspersky Endpoint Security 12.1 for Linux** application.

   The application properties window opens.

6. Go to the **Application settings** tab.

7. Go to **Detection and Response** → **Endpoint Detection and Response Optimum** section.

8. Under **Network isolation**, click **Configure device unblocking**.

9. This opens the **Configure device unblocking** window; in that window, specify the device unblocking settings.

Device unblocking settings

Setting	Description
Unblock an automatically isolated device after:	This check box enables or disables automatic unblocking of an isolated device after the time period specified in the **Hours** input field. The check box is selected by default.
Hours	Input field for the amount of time (in hours) after which an isolated device will be automatically unblocked. This field is active only if the **Unblock an automatically isolated device after** check box is selected.

10. Save your changes.

Configuring the automatic disabling of network isolation in the policy properties

To configure the automatic disabling of device network isolation:

1. In the main window of the Web Console or Kaspersky Security Center Cloud Console, select **Assets (Devices)** → **Policies and profiles**.

   The list of policies opens.

2. Select the administration group containing the devices to which the policy is applied. To do so, click the link in the **Current path** field in the upper part of the window and select the administration group in the window that opens.

   The list displays the policies configured for the selected administration group.

3. Click the name of the required policy in the list.

   The policy properties window opens.

4. Go to the **Application settings** tab.

5. Go to **Detection and Response** → **Endpoint Detection and Response Optimum** section.

6. Under **Network isolation**, click **Configure device unblocking**.

7. This opens the **Configure device unblocking** window; in that window, specify the device unblocking settings.

Device unblocking settings

Setting	Description
Unblock an automatically isolated device after:	This check box enables or disables automatic unblocking of an isolated device after the time period specified in the **Hours** input field. The check box is selected by default.
Hours	Input field for the amount of time (in hours) after which an isolated device will be automatically unblocked. This field is active only if the **Unblock an automatically isolated device after** check box is selected.

8. Save your changes.

Disabling network isolation of a device in the command line

To disable network isolation for a device using the command line, run the following command:

```
kesl-control [-R] --isolation-off
```

You can check the network isolation status and view the list of network isolation exclusions using the following command:

```
kesl-control [-R] --isolation-stat
```

One of the following network isolation statuses is displayed on the command line:

- *Network isolation enabled*.
- *Network isolation disabled*.

Configuring network isolation exclusions

You can configure exclusions:

- In the policy properties
- In the device properties

Network connections that are covered by the configured rules remain unblocked on the device after network isolation is enabled.

By default, network profiles consisting of rules that ensure uninterrupted operation of devices with the DNS/DHCP server and DNS/DHCP client roles are excluded from network isolation.

Exclusions defined in policy properties are applied only if network isolation is automatically enabled by the application as a result of reacting to the detection of indicators of compromise (IOC).

Exclusions defined in device properties are applied only if network isolation is manually enabled in the device properties or in the alert details window.

An active policy does not prevent the network isolation exclusions defined in the device properties from being applied.

You can view the list of network isolation exclusions:

- In the policy properties (**Application settings** → **Detection and Response** → **Endpoint Detection and Response Optimum** → **Exclusions** link)
- In the device properties (**Assets (Devices)** → **Managed devices** → <device name> link → <name of the Kaspersky Endpoint Security 12.1 for Linux application> link → **Application settings** → **Detection and Response** → **Endpoint Detection and Response Optimum** → **Exclusions** link)
- in the command line

Adding or removing network isolation exclusions in policy properties in the Web Console

In the Web Console or Kaspersky Security Center Cloud Console, you can add and remove network isolation exclusions in the policy properties (**Application settings** → **Detection and Response** → **Endpoint Detection and Response Optimum** → **Exclusions** link).

In the **Exclusions** window, you can click the buttons above the table to perform the following actions:

- Add information about the excluded network connection in one of the following ways:
  - Click **Add** and enter information about the network connection
  - Click **Add from profile** and select a network profile from the dictionary
- Delete information about the network connection

Adding or removing a network isolation exclusion in device properties

Adding or removing network isolation exclusions in the device properties is not available if a policy is applied to the device.

To add or remove a network isolation exclusion in the device properties:

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 the name of the **Kaspersky Endpoint Security 12.1 for Linux** application.

   The application properties window opens.

6. Go to the **Application settings** tab.

7. Go to **Detection and Response** → **Endpoint Detection and Response Optimum** section.

8. Under **Network isolation**, click **Exclusions** to open the **Exclusions** window.

9. 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 that you want to delete and click **Delete**.

10. Save your changes.

Adding network isolation exclusion window

In this window, you can enter information about a network connection that you do not want to be blocked when network isolation is enabled.

Network connection settings

Setting	Description
Name	The name of the network connection.
Direction	Direction of the network connection
Protocol	The protocol used by the network connection.
Number	The number of the network connection.
Local port(s) / range(s)	Local port numbers or ranges.
Remote port(s) / range(s)	Remote port numbers or ranges.
Remote address	IP address of the remote device

The Network profiles dictionary window

In this window, you can select the profile of a network connection to be excluded.

Network connection profiles

Network connection profile	Description
DNS server	The service providing DNS name resolution by responding to requests to get IP addresses and requests to update DNS records.
DNS client	The service providing DNS name resolution by executing DNS name queries.
Active Directory Certificate Services	Services used to create, verify, and revoke public key certificates for internal use within the organization.
Active Directory Federation Services	Services used for granting users access to multiple web services or network resources through unified sets of credentials that are stored centrally.
Active Directory Lightweight Directory Services	Services that provide the same functionality as Active Directory domain services, but do not require creating domains or domain controllers.
Active Directory Rights Management Services	Services used for controlling user access to documents.
DHCP	The service uses Dynamic Host Configuration Protocol (DHCP) to automatically allocate IP addresses.
File Transfer Protocol (FTP)	Standard network protocol for transferring files between a client and a server across a network.
Kerberos Key Distribution Center	The network service used to provide tickets (TGS) and temporary session keys to users and devices in an Active Directory domain.
Secure Shell (SSH)	A protocol that allows remote control of an operating system and tunneling of TCP connections.
Linux system components	Linux system components.

Start process

You can use the *Start process* task to remotely start processes and executable files on devices.

For example, you can run:

- Processes stopped as a result of malicious activity on the device.
- Processes stopped by you.

  For example, you can remotely start a process that you have stopped using the Terminating a process *task*.
- Scripts.

  For example, you can run a script to collect data from the device to investigate a threat.
- Utilities.

For example, you can run a utility that saves device configuration information to a file.

- Applications.

If SELinux is installed in your operating system in `Enforcing` mode, starting the *Start process* task requires additional configuration of SELinux.

You can create and run a *Start process* task as well as change its settings in the Web Console or Kaspersky Security Center Cloud Console.

You cannot create, run, or configure the *Start process* task using the command line. *Start process* tasks created in the Web Console or Kaspersky Security Center Cloud Console cannot be viewed using the `kesl-control --get-task-list` command in the command line.

Start process task settings

Setting	Description
Executable command	Field for entering the command to start the process. For example, if you want to run the `klnagchk` tool, which checks the connection to the Administration Server, you need to enter the `/<directory name>/klnagchk` command and then fill in the other fields described in the table below. You can also enter the directory name in the **Working directory path (optional)** field. In that case, do not enter the directory name in the **Executable command** field.
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 klnagchk.log` argument. This argument tells the tool to save the result to a file named `klnagchk.log`. If you need to pass multiple arguments, separate them with spaces. For example, you can enter `-logfile klnagchk.log -savecert certificate.cer` arguments. These arguments tell the tool to save the result to a file named `klnagchk.log`, and to save the certificate used to check access to the Administration Server in the `certificate.cer` file.
Working directory path (optional)	Field for entering the path to the working directory where the executable file of the script, utility, or application is located. For example, you can enter `/opt/kaspersky/klnagent64/bin/`. If you entered a directory name in the **Executable command** field, do not fill in the **Working directory path (optional)** field.

You can view the result of the task in the **Assets (Devices)** → **Tasks** → <task name> section, on the **Results** tab in the **Description** column.

Terminate process

You can remotely terminate processes on the device using the *Terminating a process* task.

For example, you can terminate:

- Processes started on a device as a result of malicious activity.
- Processes started by you.

  For example, you can remotely terminate a process that you have started using the *Start process* task.
- Scripts.

  For example, you can remotely terminate a script that you have started using the *Start process* task.
- Utilities.

  For example, you can remotely terminate an internet speed test utility that you started using the *Start process* task.
- Applications.

You cannot terminate processes of System Critical Objects (SCOs). SCOs include files that are necessary for the operation of the operating system and the Kaspersky Endpoint Security application.

You can create and run a *Terminate process* task as well as change its settings in the Web Console or Kaspersky Security Center Cloud Console. You cannot create, run, or configure the *Terminating a process* task on the command line. *Terminate process* tasks created in the Web Console or Kaspersky Security Center Cloud Console cannot be viewed using the `kesl-control --get-task-list` command in the command line.

Terminating a process task settings

Setting	Description
Specify the file whose processes you want to terminate	In the drop-down list, you can select how to specify the path to the file: • **By path to directory and checksum** • **By full path** • **By PID**. The **By PID** value is present in the drop-down list only for tasks created in device properties.
Full path to file	Field for entering the full path to the file. This field is displayed only if in the **Specify the file whose processes you want to terminate** drop-down list, you selected **By full path**.
Checksum type	In the drop-down list, you can select the file checksum type: • **MD5**. • **SHA256**.

	This drop-down list appears only if you select **By path to directory and checksum** in the **Specify the file whose processes you want to terminate** drop-down list.
File checksum	Field for entering the file checksum. This field is displayed only if in the **Specify the file whose processes you want to terminate** drop-down list, you selected **By path to directory and checksum**, and in the **Checksum type** drop-down list, you selected **MD5**.
Directory path	Field for entering the path to the directory of the file. This field is displayed only if in the **Specify the file whose processes you want to terminate** drop-down list, you selected **By path to directory and checksum**.
Process ID	Process ID (PID) entry field. This field is displayed only if in the **Specify the file whose processes you want to terminate** drop-down list, you selected **By PID**.

You can view the result of the task in the **Assets (Devices)** → **Tasks** → <task name> section, on the **Results** tab in the **Description** column.

Receiving a file from a device

You can receive files from users' devices using the *Receive file from device* task.

For example, you can receive an event log file that was generated by a third-party application.

You can create and run a *Receive file from device* task as well as change its settings in the Web Console or Kaspersky Security Center Cloud Console.

You cannot create, run, or configure the *Receiving a file from a device* task on the command line. *Receive file from device* tasks created in the Web Console or Kaspersky Security Center Cloud Console cannot be viewed using the `kesl-control --get-task-list` command in the command line.

The **Receive a file** table on the **Application settings** tab contains the following columns:

- **Directory path**.

  The path to the directory of a file on the device.

- **Checksum verification type**.

  The checksum verification type of a file on the device.

You can click the buttons above the table to add, edit, or delete data of files on the device. The *Receive file from device* task is performed for files selected in the **Receive a file** table.

Clicking the **Add** button opens the **Receive a file** window in which you can configure the settings of the *Receive file from device* task.

Receiving a file from a device task settings

Setting	Description
Specify the file to receive	In the drop-down list, you can select how to specify the path to the file: • **By path to directory and checksum** • **By full path**
Full path to file	Field for entering the full path to the file. This field is displayed only if in the **Specify the file to receive** drop-down list, you selected **By full path**.
Checksum type	In the drop-down list, you can select the file checksum type: • **MD5**. • **SHA256**. This drop-down list appears only if you select **By path to directory and checksum** in the **Specify the file to receive** drop-down list.
File checksum	Field for entering the file checksum. This field is displayed only if in the **Specify the file to receive** drop-down list, you selected **By path to directory and checksum**.
Path to file directory	Field for entering the path to the directory of the file. This field is displayed only if in the **Specify the file to receive** drop-down list, you selected **By path to directory and checksum**.

As a result of the *Receiving a file from a device* task, a copy of the file is saved in Backup on the device. You can download this copy from Backup via the Web Console or Kaspersky Security Center Cloud Console to the device from which you initiated the download.

The file size must not exceed 100 MB.

The original file on the user device remains in its original directory.

All files received through the *Receive file from device* task will have the *Infected* status in Kaspersky Security Center Backup regardless of the file scan results.

You can view the result of the task in the **Assets (Devices)** → **Tasks** → <task name> section, on the **Results** tab in the **Description** column.

Deleting a file from a device

You can delete files from a device using the *Delete file from device* task. This may be necessary, for example, as part of threat response.

System Critical Objects (SCOs) cannot be deleted. SCOs include files that are necessary for the operation of the operating system and the Kaspersky Endpoint Security application.

You can create and run a *Delete file from device* task as well as change its settings in the Web Console or Kaspersky Security Center Cloud Console.

You cannot create, run, or configure the *Deleting a file from a device* task on the command line. *Delete file from device* tasks created in the Web Console or Kaspersky Security Center Cloud Console cannot be viewed using the `kesl-control --get-task-list` command in the command line.

Deleting a file from a device task settings

Setting	Description
Specify the file to be deleted	In the drop-down list, you can select how to specify the path to the file to be deleted: • **By path and checksum** • **By full path**
Full path to file	Field for entering the full path to the file to be deleted. This field is displayed only if in the **Specify the file to be deleted** drop-down list, you selected **By full path**.
Checksum type	In the drop-down list, you can select the type of the checksum of the file to be deleted: • **MD5**. • **SHA256**. This drop-down list appears only if you select **By path to directory and** checksum in the **Specify the file to be deleted** drop-down list.
File checksum	Field for entering the checksum of the file to be deleted. This field is displayed only if in the **Specify the file to be deleted** drop-down list, you selected **By path and checksum**.
Directory path	Field for entering the path to the directory of the file to be deleted.

	This field is displayed only if in the **Specify the file to be deleted** drop-down list, you selected **By path and checksum**.
Include subdirectories	This check box enables or disables subdirectories.

If the file is blocked by another process, the task is displayed with the *Completed* status, but the file itself is deleted only after the device is restarted. After restarting the device, make sure that the file was deleted.

If you are trying to delete a running executable file, the *Deleting a file from a device* task may finish with an *Access denied* error. Create and run the *Terminating a process* task for that file, then try again.

You can view the result of the task in the **Assets (Devices)** → **Tasks** → <task name> section, on the **Results** tab in the **Description** column.

Integration with Kaspersky Managed Detection and Response

The Kaspersky Managed Detection and Response service continuously searches for, detects, and eliminates threats aimed at your organization. Integration with the Kaspersky Managed Detection and Response solution is facilitated by a Kaspersky Endpoint Security component: Managed Detection and Response (MDR).

When interacting with Kaspersky Managed Detection and Response, Kaspersky Endpoint Security can carry out the following functions:

- Send telemetry data to Kaspersky Managed Detection and Response for threat detection.
- Execute Kaspersky Managed Detection and Response commands for providing security features.

To configure integration between Kaspersky Endpoint Security and Kaspersky Managed Detection and Response, perform the following actions:

- Make sure that File Threat Protection and Behavior Detection are enabled. If these components are disabled, the device will have a red status in Kaspersky Managed Detection and Response.

  We also recommend enabling Web Threat Protection and Network Threat Protection. If these components are disabled, the device will have a yellow status in Kaspersky Managed Detection and Response.

  See the Kaspersky Managed Detection and Response Help for more information about device statuses.

- Enable the use of Kaspersky Security Network in the extended mode.

  You can enable Kaspersky Security Network in the command line, in the Web Console, or in the Administration Console.

- Configure Kaspersky Private Security Network. KPSN is required for sending telemetry.

  You can configure Kaspersky Private Security Network only in the Web Console or in the Administration Console.

  > There is no way to configure KPSN with Kaspersky Endpoint Security commands.

- Enable the Kaspersky Managed Detection and Response component and upload a BLOB configuration file, which is located in the ZIP archive of the MDR configuration file.

You can enable the Managed Detection and Response component and upload the BLOB configuration file in the command line, in the Web Console, or in the Administration Console.

Configuring KPSN to enable Kaspersky Managed Detection and Response integration

You can configure Kaspersky Private Security Network for integration with Kaspersky Managed Detection and Response only in the Web Console or in the Administration Console.

To configure KPSN, upload the Kaspersky Security Network .pkcs7 configuration file from the ZIP archive of the MDR configuration file to the Kaspersky Security Center Administration Server.

By downloading the Kaspersky Security Network 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.

To configure KPSN for integrating with Kaspersky Managed Detection and Response 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 Kaspersky Security Network .pkcs7 configuration file and click **Open**.
8. Click **Save**.

To configure KPSN for integrating with Kaspersky Managed Detection and Response in the Administration Console:

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 Private KSN** 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 Kaspersky Security Network .pkcs7 configuration file and click **Open**.

8. Click **Apply**.

Configuring the Kaspersky Managed Detection and Response integration in the Web Console

In the Web Console, you can enable or disable the integration of Kaspersky Endpoint Security with Kaspersky Managed Detection and Response and load a BLOB configuration file in the policy properties (**Application settings → Detection and Response → Managed Detection and Response**).

MDR integration settings

Setting	Description
Managed Detection and Response enabled / disabled	The toggle switch enables or disables the Managed Detection and Response component, which is necessary for integrating Kaspersky Endpoint Security with the Kaspersky Managed Detection and Response solution. The toggle button is switched off by default.
Download	Clicking this button opens a standard window in which you can select the BLOB configuration file.

The BLOB configuration file can be found inside the ZIP archive included in the Kaspersky Managed Detection and Response distribution kit.

By downloading the BLOB 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 help section.

Configuring the Kaspersky Managed Detection and Response integration in the Administration Console

In the Administration Console, you can enable or disable the integration of Kaspersky Endpoint Security with Kaspersky Managed Detection and Response and load a BLOB configuration file in the policy properties (**Detection and Response → Managed Detection and Response**).

MDR integration settings

Setting	Description
Enable Managed Detection and Response	The check box enables the Managed Detection and Response component, which is necessary for integrating Kaspersky Endpoint Security with the Kaspersky Managed Detection and Response solution. This check box is cleared by default.
Download	Clicking this button opens a standard Microsoft Windows window, where you can select the BLOB configuration file.

The BLOB configuration file can be found inside the ZIP archive included in the Kaspersky Managed Detection and Response distribution kit.

By downloading the BLOB 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 help section.

Configuring the Kaspersky Managed Detection and Response integration on the command line

In the command line, you can do the following:

- Enable or disable the Managed Detection and Response component.
- Upload or delete the BLOB configuration file required for the integration.
- Edit the start time of the *Mdr_Autostart_Scan* service task created automatically after Kaspersky Endpoint Security successfully integrates with Managed Detection and Response.

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 Managed Detection and Response component using the `UseMDR` parameter in the general application settings. You can edit the setting using command line options or a configuration file that contains all general application settings.

`UseMDR` accepts the following values:

- `Yes` to enable the Managed Detection and Response component.
- `No` to disable the Managed Detection and Response component.

You can upload or delete the BLOB configuration file via the license key management commands.

To load the BLOB configuration file, execute the following command:

```
kesl-control --load-mdr-blob <path to MDR BLOB configuration file>
```

To remove the BLOB configuration 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. You can set the start time if needed. No other task settings or schedule options can be edited.

Configuring settings for using the application in Light Agent mode

The settings described in this section apply only if Kaspersky Endpoint Security is used in Light Agent mode for protecting virtual environments.

Running Kaspersky Endpoint Security in Light Agent mode requires constant interaction between the Light Agent and the Protection Server installed on the SVM. If there is no connection to the Protection Server, the Light Agent cannot transfer file fragments to the Protection Server for scanning, and scanning is not performed.

To interact with the Protection Server, the Light Agent establishes and maintains a connection to the SVM on which this Protection Server is installed.

You can configure the settings for connecting Light Agent to SVMs in the Web Console or Administration Console. You cannot configure the settings in the command line; you can only view information about application usage in Light Agent mode.

You can configure the following settings for connecting the Light Agent to the SVM:

- SVM detection method. You can select a method that Light Agents will use to discover SVMs available to connect to. The Light Agent can discover SVMs running on the network in one of the following ways:
  - Using the Integration Server. SVMs transmit information about themselves to the Integration Server. The Integration Server generates a list of SVMs available for connection and provides it to Light Agents.

    To use this method of detecting SVMs, you need to connect SVMs and Light Agents to the Integration Server.
  - Using a list of SVM addresses. You can specify a list of SVM addresses to which Light Agents can connect.
- Algorithm for selecting SVMs to connect to. After receiving information about available SVMs, the Light Agent selects the optimal SVM to connect to in accordance with the SVM selection algorithm. You can specify which algorithm Light Agents should use when selecting an SVM to connect to.
- Connection tags. You can use connection tags to control Light Agents' connection to SVMs. If you use connection tags, Light Agent can only connect to SVMs that are configured to use that connection tag.
- Security of the connection between the Light Agent and the Protection Server. You can use encryption to protect the connection between Light Agents and Protection Servers.

For more information about the settings for connecting the Light Agent to the SVM, refer to the Help for Kaspersky Hybrid Cloud Security for Virtualization Light Agent.

Configuring Light Agent settings in the Web Console

In the Web Console, you can configure settings for connecting Light Agent to SVMs in the policy properties (**Application settings** → **Light Agent mode**).

SVM discovery settings

The settings described in this section apply only if Kaspersky Endpoint Security is used in Light Agent mode for protecting virtual environments.

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 connection of 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 SVM addresses	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 multiple IP addresses or FQDNs of SVMs on 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 advanced 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 SVM path**. If any other value is set, Light Agents will not be able to connect to the SVM.

Integration Server connection settings

The settings described in this section apply only if Kaspersky Endpoint Security is used in Light Agent mode for protecting 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 a NetBIOS name, "localhost", or 127.0.0.1 is specified as the address, the connection to the Integration Server fails with an error.
Port	Port for connecting to the Integration Server. Port 7271 is used by default.
Check	When you click the button, the web plug-in checks the SSL certificate received from the Integration Server. The button is available after entering the address and port for connecting to the Integration Server. If the certificate contains an error or is not trusted, a corresponding message is displayed in the **Connection to the Integration Server** window.
View the received certificate	Click the line to view information about the certificate received from the Integration Server.
Ignore	Select this option to save the received certificate and continue connecting to the Integration Server. If you encounter problems with an SSL certificate, we recommend to make sure that the data transmission channel you are using is secure.
Cancel	Select this option to terminate the connection to the Integration Server.
Password	Password for the Integration Server administrator account (admin account password). It is recommended to make sure that the password complexity and anti-bruteforce mechanisms ensure that the password cannot be guessed within 6 months.
Check	Clicking the button connects the web plug-in to the Integration Server.

	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. The password is stored in encrypted form.

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 tags for connecting Light Agents	The checkbox enables or disables the Light Agent's use of SVM connection tags.
Tag	A tag that is assigned to Light Agents. You can enter a text string of up to 255 characters as a tag. You can use any character except the `;` character. This entry field is available if the **Use tags for connecting Light Agents** checkbox is selected.

SVM selection algorithm

In this window, you can specify which SVM selection algorithm Light Agents for Linux should use, and configure the settings for using the advanced 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 there are no local SVMs available for connection, the Light Agent selects the SVM that has the fewest Light Agents connected, regardless of the location 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.
SVM	Allows you to specify the type of SVM path in the virtual infrastructure, which is taken into

path	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 (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux or Numa vServer). ◦ The SVM is located in the same Server Group as the virtual machine with the Light Agent installed (in a virtual infrastructure managed by the OpenStack platform, VK Cloud or the TIONIX Cloud Platform). 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 (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux or Numa vServer). ◦ The SVM is deployed in the same OpenStack project as the virtual machine with the Light Agent installed (in a virtual infrastructure managed by the OpenStack platform, VK Cloud or the TIONIX Cloud Platform). 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 (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux or Numa vServer). ◦ The SVM is located in the same Availability Zone as the virtual machine with the Light Agent installed (in a virtual infrastructure managed by the OpenStack platform, VK Cloud or the TIONIX Cloud Platform). 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 SVM path**. 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 advanced 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 need to set the **SVM path** setting to **Ignore SVM path**. 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, a secure 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.

Configuring Light Agent settings in the Administration Console

In the Administration Console, you can configure 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 for protecting 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 a NetBIOS name, "localhost", or 127.0.0.1 is specified as the address, the connection to the Integration Server fails with an error.
Port	Port for connecting to the Integration Server. Port 7271 is used by default.

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 for protecting virtual environments.

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	A list of IP addresses in IPv4 format or fully qualified domain names (FQDNs) of the SVMs to which Light Agents managed 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 multiple IP addresses or FQDNs of SVMs on 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 advanced 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 SVM path**. 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 tags for connecting Light Agents	The checkbox enables or disables the Light Agent's use of SVM connection tags.
Tag	A tag that is assigned to Light Agents. You can enter a text string of up to 255 characters as a tag. You can use any character except the `;` character. This entry field is available if the **Use tags for connecting Light Agents** checkbox is selected.

SVM selection algorithm

In this window, you can specify which SVM selection algorithm Light Agents for Linux should use, and configure the settings for using the advanced 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 there are no local SVMs available for connection, the Light Agent selects the SVM that has the fewest Light Agents connected, regardless of the location 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.
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 (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux or Numa vServer).

- The SVM is located in the same Server Group as the virtual machine with the Light Agent installed (in a virtual infrastructure managed by the OpenStack platform, VK Cloud or the TIONIX Cloud Platform).

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 (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux or Numa vServer).

  - The SVM is deployed in the same OpenStack project as the virtual machine with the Light Agent installed (in a virtual infrastructure managed by the OpenStack platform, VK Cloud or the TIONIX Cloud Platform).

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 (Skala-R), HUAWEI FusionSphere, Nutanix Acropolis, Alt Virtualization Server, Astra Linux or Numa vServer).

  - The SVM is located in the same Availability Zone as the virtual machine with the Light Agent installed (in a virtual infrastructure managed by the OpenStack platform, VK Cloud or the TIONIX Cloud Platform).

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 SVM path**. 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 advanced 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 need to set the **SVM path** setting to **Ignore SVM path**. 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, a secure 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.

Viewing information about application usage in Light Agent mode in the command line

In the command line, you can view the following information about using the application in Light Agent mode for protecting virtual environments:

- Settings for using the application in Light Agent mode
- Connecting the Light Agent to the Integration Server
- Connecting the Light Agent to SVMs

To view information about the settings for using the application in Light Agent mode, run:

```
kesl-control [-V] --ksvla-info
```

The command outputs the following information to the console:

- Light Agent mode for protecting virtual environments: enabled/disabled.

  If Light Agent mode is enabled, the application is used as a Light Agent as part of Kaspersky Hybrid Cloud Security for Virtualization Light Agent. If Light Agent mode is disabled, the application is used in Standard mode.

- VDI protection mode: enabled/disabled.

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.

- Type of protected virtual machine: temporary or persistent.
- The role of the protected virtual machine in the virtual infrastructure: server or workstation.
- The identifier (UUID) of the protected virtual machine.

To view information about connecting Light Agent to the Integration Server, run:

```
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.

To view information about connecting Light Agent to SVMs, run:

```
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.
- Method that the Light Agent uses to detect SVMs: using the Integration Server or using a list of manually defined 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 advanced 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.

Viewing events and reports

While the application is running, various *events* can occur. The events may be informational or may contain important data. For example, the application can use events to notify about a successful application database update, or to inform about an error in the operation of application components that must be eliminated.

Kaspersky Endpoint Security saves information about application events to the following logs:

- The application event log. By default, the application saves information about events to the database at /var/opt/kaspersky/kesl/private/storage/events.db. 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
- In application pop-up windows if using the Kaspersky Endpoint Security graphical user interface

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).

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.

- Application reports are available in the Kaspersky Endpoint Security graphical user interface.

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
- Web addresses of the repositories
- File names, paths to files, and hash-sums of executable application files
- Application category names

Configuring event logging to the operating system log

By default, events that occur during the operation of Kaspersky Endpoint Security are not recorded in the operating system log. You can enable the recording of events to this log using the Web Console, Administration Console, or the command line.

In Kaspersky Security Center, you can also select events to be saved to the operating system log.

Configuring in the Web Console

In the Web Console, you can configure logging events to the operating system log in the policy properties (**Application settings** → **General settings** → **Application settings**).

Clicking the **Configure notifications** link in the **Notifications** section opens the **Notifications** window. In this window, you can use the check boxes to select the events that the application records in the operating system log.

You can select individual event types or all event types with a certain severity level.

All check boxes are cleared by default.

Configuring in the Administration Console

In the Administration Console, you can configure logging events to the operating system log in the policy properties (**General settings** → **Application settings**).

Clicking **Configure** under **Notifications** opens the **Notification settings** window. In this window, you can use the check boxes to select the events that the application records in the operating system log.

You can select individual event types or all event types with a certain severity level.

All check boxes are cleared by default.

Configuring in 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.

`UseSyslog` accepts the following values:

- `Yes`: enable saving 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. You can define the following application event log options in the command line via the general application settings:

- Change the path to the application event log database via the `EventsStoragePath` option. 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. When the specified number of events is exceeded, the application deletes the oldest events.

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.

Viewing events in Kaspersky Security Center

A list of all Kaspersky Endpoint Security events is displayed in the Web Console and in the Administration Console.

You can configure event notifications. A *notification* is a message containing information about an event that occurred on a protected device. 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 command line

In the command line, you can view:

- Current application events
- Events in the application event log

Displaying current events

You can output information about all current application events or about current events associated with starting or stopping a specified task. You can use the filter to output certain current events, for example, events of a specified type.

To output information about all current application events, run:

```
kesl-control -W
```

The command returns the name of the event and additional information about the event.

To output only information about current events associated with a running task, run:

```
kesl-control --start-task <task ID/name> -W
```

Example:
Enable display of the current events of the running task with ID=1:

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

To output information about current events that match the filter conditions, run:

```
kesl-control -W --query "<filter conditions>"
```

filter conditions are set with one or more logical expressions in the format `<field> <comparison operator> '<value>'`, combined with the help of the logical operator `and`.

Example:
Display TaskStateChanged events:

```
kesl-control -W --query "EventType == 'TaskStateChanged'"
```

Example:
Display TaskSettingsChanged events initiated by the 'User' user:

```
kesl-control -W --query "EventType == 'TaskSettingsChanged' and Initiator == 'User'""
```

Displaying events from the event log

You can output information about events from the application event log to the console or a file. You can use a filter to display only certain events.

To output information about all events in the application event log, run:

```
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 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 `global application setting`.

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.

If the event log is located in the default database, you can output information about all events using the command:

```
kesl-control -E
```

To output information about events in the application event log that meet certain criteria, run:

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] [--json] [--reverse]
```

where:

- `<filter conditions>`: one or several logical expressions in the format `<field> <comparison operator> '<value>'`, combined with the help of the logical operator `and` to limit the results.
- `<number>` – number of the latest events of the selection (number of records from the end of the selection) to be displayed.
- `--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).

To output information about events in the application event log that meet certain criteria to a file, run:

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] --file <file name and path> [--json]
```

where `--file <file name and path>` is the full path to the file to output events to.

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. Intruders can replace one or more application executable modules or files with other files containing malicious code. To prevent the replacement of modules and files, Kaspersky Endpoint Security can check integrity of the 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 administration plug-in

The application 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 name of the manifest file is the same for each component, but the content of the manifest files differs. The manifest files are digitally signed and their integrity is checked as well.

The integrity of the application components is checked using an integrity check utility.

The integrity check utility must be run under the account with root privileges.

To check integrity, you can use either the utility installed with the application or the utility distributed on a certified CD.

It is recommended to run the integrity check utility from a certified CD to ensure integrity of the utility. When running the utility from the CD, specify the full path to the manifest file.

The integrity check utility installed with the application is located at the following paths:

- To check the application package, graphical user interface package, and the Network Agent: /opt/kaspersky/kesl/bin/integrity_checker.
- To check Kaspersky Endpoint Security administration plug-in – the directory where the executable modules (DLL) of the administration plug-in are located:
  - %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plug-in version>.plg\integrity_checker.exe – for 32-bit operating systems
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Security Center\Plugins\kesl_<plug-in version>.plg\integrity_checker.exe – for 64-bit operating systems

The manifest files are located at the following paths:

- /opt/kaspersky/kesl/bin/integrity_check.xml – to check integrity of the application package.
- /opt/kaspersky/kesl/bin/gui_integrity_check.xml – to check integrity of the graphical user interface package.

- /opt/kaspersky/klnagent/bin/kl_file_integrity_manifest.xml – to check the Network Agent in 32-bit operating systems.
- /opt/kaspersky/klnagent64/bin/kl_file_integrity_manifest.xml – to check the Network Agent in 64-bit operating systems.

To check integrity of the application components, run the following command:

- To check the application package and graphical user interface package:

  `integrity_checker [<path to manifest file>] --signature-type kds-with-filename`

- for checking the Kaspersky Endpoint Security administration plug-in and 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>` – path to the directory containing the Certificate Revocation List.
- `--version` – display the version of the utility.
- `--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>`, where `<file name>` is the name of the file where events that happen during scans will be logged at the DEBUG level of detail.
- `--signature-type kds-with-filename` – the type of the signature to be checked (this setting is required for checking the application package, graphical user interface package, and Network Agent).
- `--single-file <file>` – scan only one file in the manifest; ignore the other objects in the manifest.

You can view description of all available integrity check utility settings in the help on the utility options by running the `integrity_checker --help` command.

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 an *IntegrityCheckFailed* event in the event log and in Kaspersky Security Center.

Application management via the graphical user interface

The graphical user interface is not supported when using Kaspersky Endpoint Security in Light Agent mode for protecting virtual environments.

You can do the following with the Kaspersky Endpoint Security graphical user interface:

- View information about device protection status.
- Enable and disable application components:
  - File Threat Protection.
  - Removable Drives Scan.
  - Web Threat Protection.
  - Network Threat Protection.
  - Anti-Cryptor.
  - Firewall Management.
  - Application Control.
  - Device Control.
  - Behavior Detection.
  - System Integrity Monitoring.
- Start and stop scan tasks:
  - Malware Scan.
  - Critical Areas Scan.
  - Container scan.
- Start and stop database update and rollback tasks.
- Run Custom Scan by clicking a file or directory that you want to scan.
- Enable and disable Kaspersky Security Network.
- View application statistics and reports.
- Manage application license keys and view information about the license under which the application is being used as well as the key associated with the license.
- View information about objects placed in Backup.
- Create application trace files.

If an application component or task is running in "Notify only" mode, the GUI of the component or task displays the warning *"Notify only" mode selected*.

Graphical user interface

Application icon in the notification area

After the Kaspersky Endpoint Security graphical user interface package is installed on the device, the application icon appears on the right side of the taskbar notification area.

The application icon acts as a shortcut to the context menu and the main application window.

The context menu of the application icon contains the following items:

- **Kaspersky Endpoint Security 12.1 for Linux**. Opens the main application window, which displays the protection status of a device and contains interface elements that provide access to the application functions.
- **Exit**. Exits the application graphical user interface.

Main application window

To open the main application window, perform one of the following actions:

- Right-click or double-click the application icon in the notification area of the taskbar.
- Select the application name in the application menu of the operating system window manager.

The main application window is divided into several parts:

- The central part of the main application window displays the protection status of the device. Clicking this part of the window opens the **Protection Center** window. This window displays information about the protection status of a device and recommendations on the actions to be performed to fix protection problems (if any).
- The **Scan** button displays the Malware Scan task status and the number of detected threats. Clicking this button opens the **Scan** window. In this window, you can start and stop the *Malware Scan*, *Critical Areas Scan* and *Container Scan* tasks. Also, you can view reports for these tasks.
- The **Update** button displays the status of the *Update* task. Clicking this button opens the **Update** window. In this window, you can start the *Update* and *Rollback* tasks. Also, you can view reports for these tasks.
- The lower part of the main application window contains the following elements:
  - **Reports** button. Clicking this button opens the **Reports** window, where you can view component and task statistics and various reports.
  - **Backup** button. Clicking this button opens the **Backup** window, which contains information about objects in Backup.
  - **Settings** button. Clicking this button opens the **Settings** window, where you can enable or disable application components and configure the use of the Kaspersky Security Network.

- **Support** button. Clicking this button opens the **Support** window, which displays the current version of the application and the following information:

  - **Key** – the active license key added to the application, or a message that no key has been added. Clicking the link in this field opens the **License** window, which displays detailed license information.

  - **Key status** – information about the status of the active license key, or a message 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.

  The lower part of the window displays links to Kaspersky information resources and a link that opens the **Tracing** window. In this window, you can create application trace files and configure the level of detail of the trace files.

- The lower part of the main application window displays information about the license and the key, as well as about licensing problems (if any). Clicking this area of the window opens the **License** window, which displays detailed license information.

  Clicking the **Purchase a license** button in this window opens the Kaspersky online store, where you can purchase a license. After purchasing a license, you will receive an activation code or a key file, which you will need to use to activate the application.

Enabling and disabling application components

You can use the graphical user interface to enable or disable application components. If the component is enabled, the **Disable** button is available. By default, the following components are enabled: File Threat Protection, Device Control, and Behavior Detection. The Web Threat Protection component can be enabled automatically if 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) and one of the supported browsers is detected in the system.

If a component is disabled, the **Enable** button will be available.

To enable or disable an application component:

1. Open the main application window.
2. In the lower part of the main application window, click the **Settings** button.

   The **Settings** window opens.
3. Click **Enable** or **Disable** for the component.

Starting and stopping scan tasks

To start or stop a scan task:

1. Open the main application window.
2. In the main application window, click **Scan**.

The **Scan** window will open.

3. Do one of the following:

   - 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.

   - 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.

4. To view the report on the scan task, click the **Show report** button.

When an infected object is detected or the scan task is completed, a pop-up window appears in the notification area near the application icon on the right side of the taskbar.

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}*). You can hide information about temporary tasks that are already completed by clicking the cross or by closing the **Scan** window (when switching to the main window or when exiting the application).

Starting and stopping the Update task

To start or stop an update task:

1. Open the main application window.

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.

     If the Update task finishes successfully, the **Roll back update** link becomes available, and you can roll back the last successful database update.

   - 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.

To start a rollback task:

1. Open the main application window.

2. In the main application window, select the **Update** section.

   The **Update** window opens.

3. Run the Rollback task by clicking the **Roll back update** link.

Configuring Kaspersky Security Network

Using the graphical user interface, you can enable or disable Kaspersky Security Network usage.

To enable use of Kaspersky Security Network:

1. Open the main application window.
2. In the lower part of the main application window, click the **Settings** button.

   The **Settings** window opens.
3. In the **Settings** window, select one of the following options:

   - **Extended KSN mode**, if you want to use Kaspersky Security Network, obtain 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 the **Enable** button.

   The **Using Kaspersky Security Network** window opens.
5. In the **Using Kaspersky Security Network** window, carefully read the Kaspersky Security Network Statement and select the **I confirm that I have fully read, understand, and accept the terms and conditions of the Kaspersky Security Network Statement** option.
6. Click **OK**.

   The **OK** button is not available if none of the options are selected in the **Using Kaspersky Security Network** window.

To disable use of Kaspersky Security Network:

1. Open the main application window.
2. In the lower part of the main application window, click the **Settings** button.

   The **Settings** window opens.
3. Click **Enable**.
4. In the window that opens, click the **Yes** button to decline use of Kaspersky Security Network.

Viewing reports

You can use the graphical user interface to view application reports. Reports contain information about the operation of application components and tasks.

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.

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*

Reports are displayed in the window that opens when clicking **Reports** in the lower part of the main application window.

The following reports are available in the application:

- **Statistics**. This report contains File Threat Protection and scan task statistics. You can update the displayed report by clicking the **Reload** button.
- **System audit**. This report contains information about events that occur during the application operation and during the user interaction with the application.
- **Threat protection**. This report contains 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.
  - Network Threat Protection.
  - Firewall Management.
  - Application Control.
  - Device Control.
  - Behavior Detection.
  - System Integrity Monitoring.
- **On-demand tasks**. This report contains information about events logged by scan tasks, update tasks, and system integrity checks.

To view the report:

1. Open the main application window.

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.
   A report containing a list of events is displayed in the right part of the window.
   By default, events are sorted in ascending order by the values in the **Date** column.
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.

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.
- View the selected event in a separate section.

Viewing Backup objects

You can use the graphical user interface to take the following actions on Backup objects:

- View information about objects placed in Backup on the device.
- Restore objects from Backup to their original directories.
- Remove objects from Backup. Deleted objects cannot be restored in the future.

Information about restoring and deleting objects is saved to the event log.

To view objects in Backup:

1. Open the main application window.
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.

Managing license keys

Using the graphical user interface, you can add and remove application license keys, and view information about the license under which the application is being used as well as the associated license key.

You can activate the application by adding an active license key.

Activation is the process of activating a license that allows you to use a fully functional version of the application until the license expires.

If you are using the application under a license that does not include the Kaspersky Endpoint Detection and Response Optimum functionality, then to activate this functionality, you need to add an additional Kaspersky Endpoint Detection and Response Optimum Add-on license key ("EDR Optimum key").

You can also add a reserve key to the application. The reserve key becomes active when the license associated with the active key expires or when the active key is deleted. Availability of a reserve key allows you to avoid application functionality limitation when your license expires.

A reserve license key can be added only after adding an active license key.

Adding a license key

To add an active license key to the application:

1. Open the main application window.
2. Do one of the following:
   - In the lower part of the main application window, click the area, which displays information about the license and the key.
   - In the lower part of the main application window, click the **Support** button and in the **Support** window that opens, open the **License** window using the link in the **Key** field.

   The **License** window opens. Clicking the **Purchase a license** button in this window opens the Kaspersky online store, where you can purchase a license.
3. You can activate the application under a commercial license or under a trial license.

   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 **Add Key** button and select a file with a .key extension in the window that opens.

The window displays information about the key and the license associated with it.

b. Click the **Activate** button.

To activate the application under a trial license, click the **Activate** button in the **Trial key** section. The window displays information about the trial license and the associated key.

> You can use the application under a trial license for only one trial period.

After adding an active application key, you can add a reserve key and, if required, an EDR Optimum add-on key. To start adding a reserve or add-on key, use the **Add** button in the upper part of the **License** window.

Removing a license key

To remove a license key that has been added to the application:

1. Open the main application window.
2. Do one of the following:
   - In the lower part of the main application window, click the area, which displays information about the license and the key.
   - In the lower part of the main application window, click the **Support** button and in the **Support** window that opens, open the **License** window using the link in the **Key** field.

   The **License** window opens.
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.

Viewing licensing information

To view license information:

1. Open the main application window.
2. Do one of the following:
   - In the lower part of the main application window, click the area, which displays information about the license and the key.
   - In the lower part of the main application window, click the **Support** button and in the **Support** window that opens, open the **License** window using the link in the **Key** field.

   The **License** window opens.

The window displays information about the license under which the application is being used and about the license associated with the reserve key, if a reserve key has been 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 active keys and associated licenses:

- Type of active application license, license limit, and license term.
- **Key** is the 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 in UTC format.
- **Application 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 added an active EDR Optimum key to the application, information about this key and the license associated with it is also displayed in the **Current licenses** section.

The **Reserve keys** section displays information about reserve keys and associated licenses:

- Type of reserve key, license limit, and license term associated with the key.
- **Key** is the unique alphanumeric sequence.
- **License type** – the type of license associated with the reserve key.
- **Application 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 added a reserve EDR Optimum key to the application, information about this key and the license associated with it is also displayed in the **Reserve keys** section.

Creating a trace file

You can use the graphical user interface to create application trace files and define the level of detail in these.

To create a trace file:

1. Open the main application window.
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.

   You are advised to clarify the required level of detail with a Kaspersky Technical Support specialists. The default value 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.

Kaspersky Endpoint Security container application (KESL container)

Kaspersky Endpoint Security distribution kit contains files for creating a container application ("KESL container") for embedding into external systems in order to scan container images from image repositories.

The KESL container functionality is not supported when using Kaspersky Endpoint Security in Light Agent mode for protecting virtual environments.

A KESL container lets you do the following:

- Scan images of the containers located in repositories.
- Transfer scanned images that do not contain infected objects to a trusted repository.

A deployed, activated, and configured KESL container offers the following Kaspersky Endpoint Security functional components and tasks:

- File Threat Protection
- Scan tasks:
  - Malware Scan
  - Critical Areas Scan
  - Container Scan.
- Container Monitoring

The following Kaspersky Endpoint Security additional functions are available in the KESL container:

- Activating the application with a key file or activation code.
- Updating and rolling back application databases.
- Saving copies of files in Backup on the device.

You can communicate with the KESL container via a REST API. You can also configure the KESL container via policies in Kaspersky Security Center.

For correct operation of KESL containers in Kaspersky Security Center, it is recommended to move the devices that correspond to the KESL containers to a separate administration group with its own policy. In the policy properties, all Kaspersky Endpoint Security functions and settings are available for editing, but configuring settings that are not supported in a KESL container does not affect the operation of the KESL container.

KESL containers cannot be managed using the command line.

If the KESL container was activated during deployment, and it is connected to Kaspersky Security Center with automatic license key distribution to managed devices configured, the key will not apply to the devices that correspond to the KESL containers.

Deploying and activating KESL container

Distribution package description

The distribution package contains the following files:

- docker-service-<version>.tgz – Archive with files necessary to create the image
- kesl-<version>.rpm – Kaspersky Endpoint Security installation package
- klnagent.rpm – Kaspersky Security Center Network Agent installation package

The docker-service-<version>.tgz archive contains the following files:

- kesl-service – directory of the container application files.
- Dockerfile – file for building a docker image of a version below 18.06.
- Dockerfile.1809 – file for building a docker image of a version later than 18.05.
- build.sh.example – example of a script for building an image.
- run.sh.example – example of a script for launching a KESL container.
- kesl-service.config.example – example of a container application configuration file.
- klnagent.conf.example – example of a configuration file for connecting to Kaspersky Security Center.
- readme.md – quick reference.

KESL container deployment and activation

To prepare a KESL container for use:

1. Unpack the tar -xvf docker-service-<version>.tgz archive.
2. If you want to configure the KESL container settings using Kaspersky Security Center, do the following:
   a. In the klnagent.conf.example file, specify the values of the Network Agent variables. For more information, refer to Kaspersky Security Center Help section (the *"Installing Network Agent for Linux in silent mode (with an answer file)"* section).
   b. Copy klnagent.conf.example to kesl-service/klnagent.conf.
3. Build the KESL container Docker image using the build.sh.example installation script:
   a. If you use a proxy server, specify the desired values for the COMMON_AGRS variable.
   b. If necessary, change the name of the target kesl-service image to the desired one.
   c. Copy build.sh.example to build.sh and assign an executable file attribute to it.

d. Run build.sh.

4. Make sure that the build completed successfully by executing the `docker images -a` command.

   The following command execution result is displayed:

   ```
   REPOSITORY TAG IMAGE ID CREATED SIZE
   kesl-service latest <hex> < creation time > < size >
   ```

5. Activate the KESL container in one of the following ways:

   - Using Kaspersky Security Center. To activate the KESL container, you need to add the key to the devices that correspond to the KESL containers in the Web Console or in the Administration Console.

     > For correct operation of KESL containers in Kaspersky Security Center, it is recommended to move the devices that correspond to the KESL containers to a separate administration group with its own policy. When the KESL container is stopped, these devices are automatically removed from the administration group, and the key that was used for these devices is released.

   - Using a configuration file.
   - Using an environment variable (see step 7).

6. Configure the KESL container (Configuring KESL container, KESL container settings).

7. Start the KESL container using the following command `docker run --privileged --init -p < <KESL container_port >:< device_port > \`

   ```
   -e < variable_1> -e < variable_2> ... -e < variable_n> \
   -v < mount point_1> -v < mount point_2> ... -v < mount point_n> \
   < image name >
   ```

   where:

   - `< KESL container port >` is the port of the KESL container, which must be accessible by the network from outside the KESL container.
   - `< device_port >` –is the port of the device where the KESL container is installed.

   When starting the KESL container, you can activate it with an environment variable:

   - If you are using an activation code, add the `KRAS4D_ACTIVATION='< activation code >'` option:

     ```
     docker run ... -e KRAS4D_ACTIVATION='< activation code >'
     ```

   - If you are using a key file, add the `KRAS4D_ACTIVATION='< key file >'` and `KRAS4D_KEYPATH=/root/kesl-service/keys` options:

     ```
     docker run ... -e KRAS4D_ACTIVATION='< key file >' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v < path to the directory with keys >:/root/kesl-service/keys
     ```

   You can see an example of the run command in the file run.sh.example.

Configuring KESL container

KESL container settings are initialized in several ways:

- By default (unless otherwise specified).
- From the configuration file. In this case, the values from the configuration file have a higher priority than the default values.
- The values can be passed to the KESL container upon startup as environment variables. Environment variables have a higher priority than the settings from the configuration file.
- In the scan request body. The settings in the request body have the highest priority, but they are valid only within a single request.

KESL container settings

KESL container settings and their default values are described in the following table.

KESL container settings

Setting description	Available values	Default value
Port for listening to REST API		8085

Event severity level	`debug`
	`info`
	`warning`
	`error`
	`critical`
	`noset`
		noset

Authorization key	If the `KRAS4D_XAPIKEY` setting is specified, each request is verified for the presence of the x-api-key header and if its content matches the value of the `KRAS4D_XAPIKEY` setting. If these conditions are not met, the request is rejected. If this setting is missing, verification is not performed.	

Activation code or key file	To activate a KESL container using an activation code, when running the KESL container specify the activation code in the configuration file or pass the activation code in an environment variable:
	`docker run ... -e KRAS4D_ACTIVATION='<activation code>'`
	To activate a KESL container using a key file, when running the KESL container specify the key file in the configuration file or pass the key file in an environment variable:
	`docker run ... -e KRAS4D_ACTIVATION='<key file>' -e KRAS4D_KEYPATH=/root/kesl-service/keys -v <path to the directory with keys>:/root/kesl-service/keys`
	To activate a KESL container using a key file, the /root/kesl-service/keys mount point is required.	

Additional scan settings	The optional `KRAS4D_SCANOPTIONS` setting allows you to configure the settings of the Container Scan task:	

	`docker run ... -e KRAS4D_SCANOPTIONS='<settings>'` where `<settings>` are the settings of the Container Scan task.	
Additional update settings	The optional `KRAS4D_UPDATEOPTIONS` setting allows you to configure the settings of the Update task. `docker run ... -e KRAS4D_UPDATEOPTIONS='<settings>'` where `<settings>` are the Update task settings `SourceType` and `ApplicationUpdateMode`, as well as the settings in the `CustomSources.item_#` section.	
Update the application databases when KESL container starts	By default, the application databases are downloaded to the /var/opt/kaspersky/kesl/private/updates directory when the KESL container is started. To implement the joint operation of several KESL containers with one instance of the application databases and to speed up the launch of the KESL container, it is recommended to move this directory to the device where the KESL container is installed by means of mounting: `docker run ... -v <path to database directory>:/var/opt/kaspersky/kesl/private/updates`	True
Do not process the image if it already exists in the target repository.		False
Maximum time to wait for application commands to run, in seconds		600
Maximum time to wait for application database update tasks to run, in seconds		600
Name of the KESL container configuration file		kesl-service.config

Environment variables

The following environment variables can be used to configure a KESL container:

- KRAS4D_PORT – port for listening to REST API.
- KRAS4D_LOGLEVEL – event severity level.
- KRAS4D_XAPIKEY – request authorization key.
- KRAS4D_ACTIVATION – activation code or key file name.

- KRAS4D_SCANOPTIONS – additional scan settings.
- KRAS4D_UPDATEOPTIONS – additional update settings.
- KRAS4D_FORCEUPDATE – update the application databases when KESL container starts.
- KRAS4D_SKIPIMAGEIFEXISTS – do not process the image if it already exists in the target repository.
- KRAS4D_GENERALTIMEOUT – maximum time to wait for application commands to run.
- KRAS4D_UPDTASKTIMEOUT – maximum time to wait for application database update tasks to run.
- KRAS4D_CFGNAME: name of the KESL container configuration file.

Configuration file

The KESL container configuration file uses the yaml format. To read the settings from the file, mount the /root/kesl-service/config/ path on the device where the KESL container is installed, and specify the name of the configuration file if it differs from the default one. Thus, you can specify individual configuration file for each set of KESL containers.

Example: starting a KESL container

```
docker run ... \
-e KRAS4D_CFGNAME='unique_file_name' \
-v <HOST_PATH>:/root/kesl-service/config \
kesl-service
```

The table below shows the configuration file settings and the corresponding environment variables.

Correspondence between the settings and the environment variables

Configuration file setting	Environment variable
Common section	
port: <port for listening>	# KRAS4D_PORT=8085
sqlpath: <full path to the database file that contains scan results>	# KRAS4D_SQLPATH
certdir: <path to the directory with registry certificates>	# KRAS4D_CERTDIR
keypath: <path to the directory with license keys>	# KRAS4D_KEYPATH
tmppath: <full path to the temporary directory>	# KRAS4D_TMPPATH
logpath: <full path to the event log>	# KRAS4D_LOGPATH
loglevel: [noset|debug|info|warning|error|critical]	# KRAS4D_LOGLEVEL
Control section	
xapikey: <request authorization key>	# KRAS4D_XAPIKEY=None
forceupdate: <forced database update at container start [True|False]>	# KRAS4D_FORCEUPDATE
activation: <activation code or key file name from /root/kesl-service/config/>	# KRAS4D_ACTIVATION
detectaction: [delete|skip]	# KRAS4D_DETECTACTION

scanoptions: <scan settings [ScanArchived=yes ScanSfxArchived=yes ...]>	# KRAS4D_SCANOPTIONS
skipimageifexist: <do not scan the image if it already exists on the server to which the scanned image is to be copied>	# KRAS4D_SKIPIMAGEIFEXIST
generaltimeout: <maximum time to wait for application commands to run>	# KRAS4D_GENERALTIMEOUT
updtasktimeout: <maximum time to wait for application database update tasks to run>	# KRAS4D_UPDTASKTIMEOUT
Repositories section	
<server>:<port>: address and port of the image registry that requires authorization when requesting for verification.	
Credentials subsection	
user: user name for authorization in the image registry	
pass: password for authorization in the image registry	

Example of a configuration file

```
common:
    port: 8085
    sqlpath: './data/scans.sqlite'
    tmppath: './tmp/'
    keypath: './keys/'
    certdir: './certificates/'
    logpath: '/var/log/kaspersky/kesl-service/'
    loglevel: 'debug'
control:
    xapikey: 0000
    activation: XXXX-XXXX-XXXX-XXXX or XXXX.key
    scanoptions: 'ScanArchives=yes'
    updateoptions: ''
    forceupdate: True
    skipimageifexists: False
    generaltimeout: 600
    updtasktimeout: 1000
repositories:
    repository.any.com:
        certificate: repository_any_comcert.pem
        credentials:
            user: user
            pass: password
```

Available mount points

The following mount points are available for working with the KESL container:

- /root/kesl-service/data/scans.sqlite – path to the database file that contains scan results.
- /var/opt/kaspersky/kesl/private/updates – path to the application databases.
- /root/kesl-service/certificates – path to the directory that contains repository certificates.
- /root/kesl-service/keys – path to the directory that contains license keys.
- /var/log/kaspersky/ – path to the directory that contains event logs.
- /root/kesl-service/config/ – path to the configuration files.
- /var/lib/containers/vfs-storage – required mount point for the Podman utility to work correctly.

Managing KESL container using REST API

Interaction with the KESL container is implemented using the REST API. You can use a REST API to do the following:

- Scan a file or multiple files. For this purpose, submit a scan request (POST).

  Example:
  POST http://<server>:<port>/scans

  One or multiple files.

- Scan a Docker image or multiple Docker images. For this purpose, submit a scan request (POST).

  Example:
  POST http://<server>:<port>/scans

  Link to the Docker images to scan.

- Scan a Docker image or multiple Docker images with additional settings. For this purpose, submit a scan request (POST).

  Example:
  POST http://<server>:<port>/scans

  JSON of a certain type.

- Get a list of scan sessions. For this purpose, send a request for information on scan sessions (GET).

  Example:
  GET http://<server>:<port>/scans

- Get information on a scan session. For this purpose, send a request for information on scan sessions (GET).

  Example:
  GET http://<server>:<port>/scans/<unique scan session identifier>

- Add a registry certificate without reloading the KESL container. For this purpose, submit a request for adding a registry certificate (POST).

  Example:
  POST http://<server>:<port>/addcert

- Get information about the state of the KESL container. To do this, send a request to receive information about the state of the KESL container (GET).

  Example:
  GET http://<server>:<port>/status

Scan request

Purpose

Scan of the object specified in the request body.

The following objects can be scanned:

- One file
- Multiple files
- One or multiple Docker images located in a specific repository
- One or multiple Docker images located in a specific repository with additional settings

Path

http://<server>:<port>/scans[?wait=1]

Settings

The optional `wait` setting specifies the type of the scan session.

If the setting value is `1`, synchronous scan is performed and the application sends a report when scan finishes.

If the setting value is `0`, asynchronous scan is performed, and the response is as follows:

```
{
  "id"="7d27e9b4-a4d7-469b-bdcf-ebfe953498e4",
  "location"="/scans/7d27e9b4-a4d7-469b-bdcf-ebfe953498e4"
}
```

where:

- id – unique identifier of the scan session.
- location – path for requesting information on this section: http://<server>:<port>/scans/<location>.

Request headers

The request can contain the following headers:

- Content-Type
  Defines the type of the object submitted for scan.
  Supported values:
  - application/octet-stream – one file
  - multipart/form-data – multiple files

- text/plain – one or multiple Docker images located in a specific repository
- application/json – one or multiple Docker images located in a specific repository with additional settings

- x-api-key (optional)
  API key specified in the KRAS4D_XAPIKEY environment variable or the xapikey variable in the configuration file.

Possible errors

If an unsupported value is specified in the Content-Type header, the application returns the following error:

```
{
  "error"={

"code"="NOT_SUPPORTED_CONTENT_TYPE",
"details"="<content type>",
"message"="Not supported Content-Type"
  },

  "status"="error"

}
```

Scan file request

Content-Type

application/octet-stream

Request body

File.

Response example:

```
{
  "completed": "Mon, 01 Mar 2021 06:54:39 GMT",

  "created": "Mon, 01 Mar 2021 06:54:38 GMT",

  "progress": 100,

  "scan_result": {
```

```
"noname": {
"started": "2021-03-01 06:54:39",
"stopped": "2021-03-01 06:54:39",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/b8eb4128-8cb4-4964-87cf-b9853e6544ec"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]

}
```


Request to scan multiple files

Content-Type

multipart/form-data

Request body

Multiple files.

Response example:


```
{

  "completed": "Mon, 01 Mar 2021 06:55:44 GMT",

  "created": "Mon, 01 Mar 2021 06:55:43 GMT",

  "progress": 100,

  "scan_result": {
```

```
"clean": {
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "clean"
},
"corrupted.com": {
"errors": [
{
"error": "Corrupted object",
"object": "/root/kesl-service/tmp/75d28fe6-8154-4361-9382-90a76861518a"
}
],
"started": "2021-03-01 06:55:43",
"stopped": "2021-03-01 06:55:43",
"verdict": "non scanned"
},
"error.com": {
"errors": [
{
"error": "read error",
"object": "/root/kesl-service/tmp/37f6e0dd-13f9-4d11-899c-5fe0f23e407d"
}
],
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"verdict": "non scanned"
},
"infected.com": {
"started": "2021-03-01 06:55:44",
"stopped": "2021-03-01 06:55:44",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/7d664646-bf56-4060-b958-5ce9e746c929"
}
],
"verdict": "infected"
}
  },

  "status": "completed",
```

```
  "verdicts": [

"clean",
"non scanned",
"infected"
  ]

}
```

Request to scan Docker images

Content-Type

text/plain

Request body

Link to the Docker images to scan.

The following values are available:

- Path to an image in the repository (for example, https://index.docker.io/jerbi/eicar:latest).
- Path mask for multiple images (for example, https://index.docker.io/<name mask>:<tag mask>). You can use the ? and * characters to specify a mask.

Response example:

```
{

  "completed": "Sun, 31 Jan 2021 10:29:26 GMT",

  "created": "Sun, 31 Jan 2021 10:29:20 GMT",

  "progress": 100,

  "scan_result": {

"jerbi/eicar:latest": {
"started": "2021-01-31 10:29:25",
"stopped": "2021-01-31 10:29:26",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
```

```
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"
  ]

}
```

Possible errors

A request using the Docker REST API is used to get a list of images by mask.

However, on many public servers it is disabled for security reasons. An attempt to scan images by mask on such servers results in an error.

Error example:

```
{

  "completed": "Mon, 01 Mar 2021 07:02:24 GMT",

  "created": "Mon, 01 Mar 2021 07:02:22 GMT",

  "scan_errors": [

{
"code": 401,
"details": {
"context": {
"image_mask": "/jerbi/eic*:latest",
"repository": "index.docker.io",
"repository_base": "index.docker.io"
},
"errors": [
"Unauthorized"
]
},
"message": "Invalid source"
```

```
},
[
"Unauthorized"
]
  ],

  "status": "completed"

}
```

Request to scan Docker images with additional settings

Content-Type

application/json

Request body

JSON of the following type:

```
{

  "source": "https://index.docker.io/jerbi/eicar:latest",

  "params": {

"destination": "https://fake",
"skipimageifexists": true,
"custom_callbacks": {
"on_detect": {
"uri": "http://10.16.42.75:5050",
"content-type": "application/json",
"body": {
"session_id": "100",
"session_init": "20201105T072403+0300",
"infected_items": "$infected"
}
},
"on_complete": {
"body": {
"session_id": "100",
},
```

```
"uri": "http://10.16.42.75:5050/on_complete",
}
}
  }

}
```

Additional request settings

The `params` section can contain the following settings:

- `destination` (optional) – the server to which the scanned image will be copied.
- `skipimageifexists` (optional) – do not scan or copy the image if the destination server already has an image with the same name and SHA256 hash. This setting can only be specified if the `destination` setting is specified.
- `custom_callbacks` (optional) – describes the requests that should be sent when scan finishes:
  - on_detect – the request is sent if a threat is detected.
  - on_complete – the request is always sent when scan finishes.

In the description of the request body, you can specify the `$infected` substitution variable. The list of infected objects is substituted instead of this variable.

Response example:

```
{
  "completed": "Mon, 01 Mar 2021 07:13:49 GMT",
  "created": "Mon, 01 Mar 2021 07:13:42 GMT",
  "progress": 100,
  "scan_errors": [
{
"code": 500,
"message": "Unable to get images hash from destination registry"
}
  ],
  "scan_params": {
"destination": "https://fake",
"skipimageifexists": true
```

```
  },

  "scan_result": {

"jerbi/eicar:latest": {
"started": "2021-03-01 07:13:48",
"stopped": "2021-03-01 07:13:49",
"threats": [
{
"name": "EICAR-Test-File",
"object": "[image:docker.io/jerbi/eicar:latest] /eicar.com.txt"
}
],
"verdict": "infected"
}
  },

  "status": "completed",

  "verdicts": [

"infected"

  ]

}
```

Request for information on scan sessions (GET)

Purpose

Obtaining information about the scan sessions.

Path

http://<server>:<port>/scans[?force] – request for a list of sessions.

http://<server>:<port>/scans/<unique scan session identifier>[?force] – request for information on a specific session.

Settings

The KESL container stores data about scan sessions in the memory and writes them to the scan results database.

The optional `?force` setting initiates reading information from the database if several KESL container instances are working with the same database. If this setting is missing, information will be displayed only about the sessions that were initiated by a specific KESL container instance.

Request for the list of scan sessions

Path

http://<server>:<port>/scans[?force]

Response example:

```
{
  "629ae0a9-28de-4e2f-b130-67e87ba4d61d": {
"progress": 100,
"status": "completed"
  },
  "655b96fc-34ca-4915-9c41-d52724a277de": {
"progress": 100,
"status": "completed"
  },
  "7d27e9b4-a4d7-469b-bdcf-ebfe953498e4": {
"progress": 100,
"status": "completed"
  },
  "c32ca88f-2d24-47ec-b040-0540366bea4b": {
"progress": 100,
"status": "completed"
  },
  "df11ad81-26aa-42f9-94bb-39dee4304807": {
"progress": 0,
"status": "completed"
```

```
  },

  "fa25340f-4898-497f-ab59-8df494f4ea47": {

"progress": 100,
"status": "completed"

  }

}
```

Request for information on a specific session

Path

http://<server>:<port>/scans/<unique scan session identifier>[?force]

Response example:

```
{

  "completed": "Mon, 01 Mar 2021 06:45:19 GMT",

  "created": "Mon, 01 Mar 2021 06:45:19 GMT",

  "progress": 100,

  "scan_result": {

"noname": {
"started": "2021-03-01 06:45:19",
"stopped": "2021-03-01 06:45:19",
"threats": [
{
"name": "EICAR-Test-File",
"object": "/root/kesl-service/tmp/65b55d89-b758-4609-a2f3-f63ef839815d"
}
],
"verdict": "infected"
}

  },

  "status": "completed",
```

```
  "verdicts": [

"infected"

  ]

}
```

Request for adding a registry certificate (POST)

Purpose

Adding a registry certificate without reloading the KESL container.

Path

http://<server>:<port>/addcert

Request headers

The request contains a Content-Type header.

Supported values:

- application/octet-stream – one certificate file
- multipart/form-data – multiple certificate files

Request for information about the state of a KESL container (GET)

Purpose

Obtaining information about the current state of a KESL container and the application status parameters that determine the state of the KESL container (the status of the application, license, and databases).

Path

http://<server>:<port>/status

Response example:

```
{'product info': {'databases_date': '<database release date>', 'databases_loaded':
True, 'license_expiration': '<license expiration date>', 'license_info': 'The key is
valid', 'policy': 'Not applied', 'version': '<application version>'}, 'status':
'service available'}
```

Possible errors

An example of an error (the application is not running in the KESL container):

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': 'N/A', 'license_info': 'N/A', 'policy': 'N/A', 'version':
'N/A'}, 'status': 'service not available', 'status_reason': ['KESL not response']}
```

Example of an error (application databases were not downloaded):

```
{'product info': {'databases_date': 'N/A', 'databases_loaded': False,
'license_expiration': '<license expiration date>', 'license_info': 'Inconsistent
update', 'policy': 'Not applied', 'version': '<application version>'}, 'status':
'service not available', 'status_reason': ['Databases not loaded', 'License error:
Inconsistent update']}
```

Example of an error (the license has expired):

```
{'product info': {'databases_date': '<database release date>', 'databases_loaded':
True, 'license_expiration': '<license expiration date>', 'license_info': 'Expired',
'policy': 'Not applied', 'version': '<kesl version>'}, 'status': 'service not
available', 'status_reason': ['License error: Expired']}
```

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 Kaspersky Endpoint Security for the whole duration of its life cycle (see Application life cycle). 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. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky specialists through online requests. The Kaspersky CompanyAccount portal lets you monitor the progress of electronic request processing by Kaspersky specialists and store a history of electronic requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky and also manage the privileges of these employees via 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 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.

Application trace files

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 generation of application trace files and define the level of detail in trace files in the command line via the general application settings and the graphical user interface.

If you have enabled application trace files, these will be stored at /var/log/kaspersky/kesl/. Access to this directory requires root privileges.

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.

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.
- 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.

Configuring application trace settings

If you are managing the Kaspersky Endpoint Security application through Kaspersky Security Center, you can configure trace settings of the application in the Kaspersky Endpoint Security policy settings using the Web Console or the Administration Console.

If you are managing the application on the command line, you can configure trace settings of the application in the general application settings.

Editing trace settings in the Web Console

In the Web Console, you can configure application tracing settings in the policy properties (**Application settings** → **General settings** → **Application settings**, **Trace and dump settings** section) (see the table below).

Application trace 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 account under which Kaspersky Endpoint Security is running has read/write permissions for this directory. Root privileges are required to access the default trace files directory.
Maximum number of trace files	Input field for the maximum number of application trace files. Default value: 10.
Maximum trace file size (MB)	Input field for the maximum size of an application trace (in megabytes). Default value: 500.

To apply trace settings, you must restart the application.

Editing trace settings in the Administration Console

In the Administration Console, you can configure application tracing settings in the policy properties (**General settings → Application settings**).

Under **Trace and dump settings**, click **Configure** to open a window in which you can edit the trace settings (see the table below).

Application trace 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 account under which Kaspersky Endpoint Security is running has read/write permissions for this directory. Root privileges are required to access the default trace files directory.
Maximum trace file size (MB)	Input field for the maximum size of an application trace (in megabytes). Default value: 500.
Maximum number of trace files	Input field for the maximum number of application trace files. Default value: 10.

To apply trace settings, you must restart the application.

Editing trace settings in the command line

In the command line, you can configure application tracing settings using the `TraceLevel`, `TraceFolder`, `TraceMaxFileCount` and `TraceMaxFileSize` settings in general application settings.

The `TraceLevel` setting lets you enable or disable application tracing and specify the level of detail in trace files. This setting can take the following values:

- `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.
- `None` (default value) — Do not generate a trace file.

The `TraceFolder` settings lets you specify the directory where application trace files are stored. Default value: /var/log/kaspersky/kesl. If you specify a different directory, make sure that the account under which Kaspersky Endpoint Security is running has read/write permissions for this directory. Root privileges are required to access the default trace files directory.

`TraceMaxFileCount` lets you specify the maximum number of application trace files. The setting can take values from 1 to 10000. Default value: 10.

`TraceMaxFileSize` lets you specify the maximum size of an application trace file (in megabytes). The setting can take values from 1 to 1000. Default value: 500.

You can edit the setting using command line options or a configuration file that contains all general application settings.

After changing the values of the `TraceFolder`, `TraceMaxFileCount`, or `TraceMaxFileSize` settings, you need to restart the application.

Application administration plug-in trace files

Administration plug-in 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 administration plug-in trace files

If you use the Administration Console to manage Kaspersky Endpoint Security, information about events that occur while the MMC administration 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.

Web administration plug-in trace files

If you use the Web Console to manage Kaspersky Endpoint Security, information about events that occur while the web administration 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.

Contents of administration plug-in trace files

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.

In addition to general data, trace files 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.

About dump files

A *dump file* contains all information about the working memory of Kaspersky Endpoint Security processes at the time of creating the dump No dump files are generated by default. You can enable or disable dumping in case of application failures.

If you enabled dumping, dump files are stored at /var/opt/kaspersky/kesl/common/dumps and /var/opt/kaspersky/kesl/common/dumps-user.

Root privileges are required to access dump files.

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.

Dump files may contain personal data. It is recommended to protect information from unauthorized access before sending it to Kaspersky.

Enabling or disabling dump logging

If you are managing the Kaspersky Endpoint Security application through Kaspersky Security Center, you can enable or disable dumping 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 kesl.ini configuration file.

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`.

Enabling or disabling dumping in the Web Console

In the Web Console, you can enable or disable logging dump files in the policy properties (**Application settings** → **General settings** → **Application settings**, **Trace and dump settings** section).

Dump file settings

Setting	Description
Create a dump file if the application crashes	This checkbox enables or disables 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.

You must restart the application to apply the dump file settings.

Enabling or disabling dumping in the Administration Console

In the Administration Console, you can enable or disable logging dump files in the policy properties (**General settings** → **Application settings**).

Under **Trace and dump settings**, click **Configure** to open a window in which you can edit the dumping settings.

Dump file settings

Setting	Description
Create a dump file if the application crashes	This checkbox enables or disables 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.

You must restart the application to apply the dump file settings.

Enabling or disabling dumping on the command line

To enable or disable dumping via the kesl.ini configuration file, do as follows:

1. Stop Kaspersky Endpoint Security.
2. Open the /var/opt/kaspersky/kesl/common/kesl.ini file for editing.
3. Under **[General]**, set the parameter value:
   - `CoreDumps=yes`: enable dumping in case of a failure.
   - `CoreDumps=no`: disable dumping.
4. If you want to change the default directory where dump files are saved, specify the path to the directory in the `CoreDumpsPath` option.
5. Start Kaspersky Endpoint Security.

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 its name.

   The device properties window opens.

3. On the **Advanced** tab, select the **Remote diagnostics** section.

In the remote device diagnostics window, you can view the remote application installation log.

To view the remote application installation log on a device:

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** will open.

You can use the remote device diagnostics utility to view the remote installation log.

To view the remote application installation log on a device:

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.

Manually checking the connection with the Administration Server. Klnagchk utility

The Network Agent distribution kit includes the klnagchk utility, which is intended for checking connection to the Administration Server.

After installation of the Network Agent, the utility is located in the /opt/kaspersky/klnagent/bin directory in 32-bit operating systems and in the /opt/kaspersky/klnagent64/bin directory in 64-bit operating systems. Depending on the utilized keys, the Network Agent performs the following actions when started:

- Writes to the event log file or displays the values of the settings for connecting the Network Agent installed on the client device to the Administration Server.
- Writes to the event log file or displays the Network Agent statistics (since its last launch) and the results of running the utility.
- Attempts to establish a connection between Network Agent and the Administration Server.
- If the connection fails, the utility sends an ICMP packet to check the status of the device where the Administration Server is installed.

Utility syntax

```
klnagchk [-logfile <file name>] [-sp] [-savecert <path to certificate file>] [-restart]
```

Description of keys

- `-logfile <file name>`: write to an event log file both the values of the settings for connecting Network Agent to the Administration Server and the results of running the utility. If this key is not used, the settings, results, and error messages are displayed on the screen.
- `-sp`: show the password for user authentication on the proxy server. This setting is used if the connection to the Administration Server is established via a proxy server.
- `-savecert <file name>`: save the certificate used to authenticate access to the Administration Server in the specified file.
- `-restart`: restart Network Agent.

Manually connecting to the Administration Server. Klmover utility

The Network Agent distribution kit includes the klmover utility, which is intended for managing the connection with the Administration Server.

After installation of the Network Agent, the utility is located in the /opt/kaspersky/klnagent/bin directory in 32-bit operating systems and in the /opt/kaspersky/klnagent64/bin directory in 64-bit operating systems. Depending on the utilized keys, the Network Agent performs the following actions when started:

- Connects Network Agent to the Administration Server with the specified settings.
- Writes to an event log file or displays the operation results.

Utility syntax

```
klmover [-logfile <file name>] {-address <server address>} [-pn <port number>] [-ps
<SSL port number>] [-nossl] [-cert <path to the certificate file>] [-silent] [-dupfix]
```

Description of keys

- `-logfile <file name>` – write the results of running the utility to the specified file. If this key is not used, the results and error messages are displayed in stdout.

- `-address <server address>` – address of the Administration Server used for the connection. This can be the IP address, NetBIOS, or DNS name of the device.

- `-pn <port number>` – number of the port over which a non-encrypted connection to the Administration Server is established. Port 14000 is used by default.

- `-ps <SSL port number>` – number of the SSL port over which the encrypted connection to the Administration Server is established using the SSL protocol. Port 13000 is used by default.

- `-nossl` – use a non-encrypted connection to the Administration Server. If this key is not specified, the Agent is connected to the Administration Server over the encrypted SSL protocol.

- `-cert <path to certificate file>` – use the specified certificate file for access authentication to the new Administration Server. If the key is not in use, Network Agent receives a certificate upon the first connection to the Administration Server.

- `-silent` – start the utility in non-interactive mode. Using this key may be useful if, for example, the utility is started from a startup script during user registration.

- `-dupfix` – this key is used if the Network Agent installation method differs from the installation within the distribution kit; for example, if the Network Agent was restored from a disk image.

- `-cloningmode 1` – switch to cloning mode.

- `-cloningmode 0` – switch from cloning mode.

Appendices

This section provides information that complements the primary Help text.

Appendix 1. Resource consumption optimization

When scanning objects, Kaspersky Endpoint Security uses the processor resources, disk subsystem input/output, and operating system.

To view the resource consumption by the application, execute the following command:

```
top -bn1|grep kesl
```

> The command must be executed when the system is loaded.

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%.

If Kaspersky Endpoint Security operation while scanning objects critically slows down the system, the application must be configured to optimize consumption of system resources.

Determining the task that consumes resources

To determine which application tasks are consuming system resources, it is necessary to distinguish the resource consumption of File Threat Protection tasks (OAS type) and On-demand Scan tasks (ODS and ContainerScan types).

If the application is managed by Kaspersky Security Center policy, it is required to allow local task management for the period of the study.

File Threat Protection task operation analysis

To analyze the operation of the File Threat Protection task:

1. Stop all scan and monitoring tasks.
2. Make sure that the on-demand scan tasks will not run during the scan or have no schedule. You can do it using Kaspersky Security Center or locally by doing the following steps:
    a. Get the list of all application tasks by executing the following command:

```
kesl-control --get-task-list
```

b. Get the schedule settings for the Malware Scan task by executing the following command:

```
kesl-control --get-schedule <task ID>
```

If the command output is `RuleType=Manual`, the task can only be started manually.

c. Get the schedule settings for all your Malware Scan tasks, if any, and set them to start manually by executing the following command:

```
kesl-control --set-schedule <task ID> RuleType=Manual
```

3. Enable generation of application trace files with a high level of details by executing the following command:

```
kesl-control --set-app-settings TraceLevel=Detailed
```

4. Start the File Threat Protection task if it has not been started by executing the following command:

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

5. Load the system in the mode that caused the performance problems; a few hours is enough.

While being loaded, the application writes a lot of information to the trace files; however only 5 files of 500 MB are stored by default, so the old information will be overwritten. If the problems with performance and resource consumption stop occurring, then they are most likely caused by on-demand scan tasks and you can proceed to analyzing the operation of ContainerScan and ODS scan tasks.

6. Disable creation of the application trace files by executing the following command:

```
kesl-control --set-app-settings TraceLevel=None
```

7. Determine the list of objects that have been scanned the most times by running the following command:

```
fgrep 'AVP ENTER' /var/log/kaspersky/kesl/kesl.* | awk '{print $8}' | sort | uniq -c | sort -k1 -n -r|less
```

The result is loaded into less, a text viewer utility, where the objects that have been scanned the most times are displayed first.

8. Determine whether the objects scanned the most number of times are dangerous. In case of any difficulties, contact Technical Support.

For example, directories and log files can be considered safe if a trusted process writes to them, database files can also be considered safe.

9. Write down the paths to the objects that are safe, in your opinion; the paths will be required to configure exclusions from the scan scope.

10. If various services frequently write data to files in the system, such files are scanned again in the pending queue. Determine the list of paths that have been scanned the most times in the pending queue by running the following command:

```
fgrep 'SYSCALL' /var/log/kaspersky/kesl/kesl.* | fgrep 'KLIF_ACTION_CLOSE_MODIFY' | awk '{print $9}' | sort | uniq -c | sort -k1 -n -r
```

The files that were scanned the most times will appear at the beginning of the list.

11. If the counter for a file exceeds several thousands in a few hours, you should check whether you can trust this file in order to exclude it from scan.

The logic of to determine it is the same as for the previous study (see step 8): log files can be considered safe, since they cannot be launched.

12. Even if some files are excluded from scan by the Real-time protection task, they can still be intercepted by the application. If excluding certain files from Real-time protection does not result in significant increase of performance, you can completely exclude the mount point where these files are located from the interception scope of the application. To do so, do the following:

    a. Run the following command to get the list of files intercepted by the application:

    ```
    grep 'FACACHE.*needs' /var/log/kaspersky/kesl/kesl.* | awk '{print $9}' | sort |
    uniq -c | sort -k1 -n -r
    ```

    b. Using this list, determine the paths used for most of the file operation interceptions and configure interception exceptions.

On-demand Scan tasks operation analysis

Tasks of the ODS and ContainerScan types can also cause significant resource consumption. Follow these recommendations for the tasks of ODS type:

- Make sure that several on-demand scan tasks are not running at the same time. The application allows for operation in this mode, but resource consumption can significantly increase. Check the schedule of all tasks of the ODS and ContainerScan types locally (as described for the File Threat Protection task) or using Kaspersky Security Center.
- Run the scan during the minimum server load.
- Make sure that there are no mounted remote resources (SMB/NFS) at the specified scan path. If a remote resource scan task cannot be performed directly on the server that provides the resource, do not perform the resource scan on servers with critical services, as execution of this task can take a long time (depending on the connection speed and the number of files).
- Optimize the settings of the on-demand scan task before start.

Configuring the File Threat Protection task

If, after analysis of the File Threat Protection task's operation, you have created a list of directories and files that can be excluded from the scan scope, you need to add them to the exclusions.

Scan exclusions

To exclude the /tmp/logs directory and all subdirectories and files recursively, execute the following command:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs
```

To exclude a specific file or files by mask in the /tmp/logs directory, execute the following command:

```
kesl-control --set-settings 1 --add-exclusion /tmp/logs/*.log
```

To exclude all files with the .log extension in the /tmp/ directory and subdirectories using a recursive mask, execute the following command:

```
kesl-control --set-settings 1 --add-exclusion /tmp/**/*.log
```

Interception exclusions

If you want to exclude files in a certain directory not only from scan, but also from interception, you can exclude the entire mount point.

To exclude an entire mount point:

1. If the directory is not a mount point, create a mount point from it. For example, to create a mount point from the /tmp directory, execute the following command:

   ```
   mount --bind /tmp/ /tmp
   ```

2. To keep the mount point after the server reboot, add the following line to the /etc/fstab file:

   ```
   /tmp /tmp none defaults,bind 0 0
   ```

3. Add the /tmp directory to the global exceptions by executing the following command:

   ```
   kesl-control --set-app-settings ExcludedMountPoint.item_0000=/tmp
   ```

4. If you want to add several directories, increase the item_0000 counter by one (item_0001, item_0002, and so on).

It is also recommended to exclude mount points that are mounted remote resources with unstable or slow connection.

Changing scan type

By default, the File Threat Protection task can scan files when they are opened or closed. If analysis of the File Threats Protection task performance shows that too many files are being written, you can make the task operate only when files are opened by running the following command:

```
kesl-control --set-set 1 ScanByAccessType=Open
```

In this operation mode, changes made to the file after it is opened are not scanned until the next opening of the file.

Configuring the On-demand Scan task

Scan exclusions

You can define scan exclusions for on-demand ODS and ContainerScan tasks. You can configure this in the same way as scan exclusions for the File Threat Protection task.

Scan exclusion settings for one scan task do not affect other scan tasks. Exclusions must be configured separately for each scan task.

Setting the memory usage limits when unpacking archives

The on-demand scan task uses RAM to unpack archives when scanning the archives recursively. By default, the application's limit is 40% of all available RAM, but not less than 2 GB. Therefore, if the system has more than 5 GB of RAM, you can manually set the memory usage limit. This is especially useful for the servers that have hundreds of gigabytes of RAM.

Setting the application memory usage limit

You can limit the amount of RAM that Kaspersky Endpoint Security uses when running OAS, ODS, and ContainerScan scan tasks.

The application uses no more than 40% of all available RAM by default. The memory usage limit may be useful for systems with a large amount of RAM (more than 5 GB).

You can use the `ScanMemoryLimit` option in the kesl.ini configuration file to adjust the size of RAM used by the application when scanning files. Default value: 8192 MB.

> 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.

To specify a limit on memory use when scanning files:

1. Stop Kaspersky Endpoint Security.
2. Open the /var/opt/kaspersky/kesl/common/kesl.ini file for editing.
3. Under **[General]**, specify the required amount of RAM in `ScanMemoryLimit`:

   `ScanMemoryLimit=<amount of memory in megabytes>`

   The minimum value is 2048 MB. If the value is less than 2048 MB, the application will use the minimum value.

   If you specified a value that exceeds the system RAM size, the application will use up to 40% of all available RAM.
4. Start Kaspersky Endpoint Security.

The new memory usage limit for scanning files will be in effect after the application restarts.

Appendix 2. 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 <command group prefix>`

Where `<command group prefix>` accepts 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 managing application events
- -F: commands for managing firewall
- -H: commands for managing blocked devices
- -L: commands for managing license keys
- -N: commands for managing encrypted connections scan settings
- -R: commands for managing the settings of Kaspersky Endpoint Security integration with Kaspersky Endpoint Detection and Response (KATA) and Kaspersky Endpoint Detection and Response Optimum.
- -S: statistics commands
- -T: commands for managing application tasks and settings
- -U: commands for managing users and roles
- -V: application commands in light agent mode for protecting virtual environments
- -W: event display commands

Commands for managing application tasks and settings

-T is a prefix indicating that the command belongs to the group of commands for managing application settings and tasks.

-C is a prefix indicating that the command belongs to the group of commands for managing container scan settings.

-N is a prefix indicating that the command belongs to the group of commands for managing secure connections 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.

Command syntax

```
kesl-control [-T] --export-settings [--file <configuration file path>] [--json]
```

Arguments and keys

`--file <configuration file path>` – full path to the configuration file where the application settings will be saved.

`--json` is specified to output the settings in JSON format. If the `--json` key is not specified, the settings will be imported in the INI format.

kesl-control --import-settings

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.

Command syntax

```
kesl-control [-T] --import-settings --file <configuration file path> [--json]
```

Arguments and keys

`--file <configuration file path>` – full path to the configuration file to import the settings into the application.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` key 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.

> It can only be executed if the application is being used in standard mode.

Command syntax

```
kesl-control [-T] --update-application
```

Commands for managing general application settings

The kesl-control --get-app-settings command

The command outputs the current values of the general application settings to the console or a configuration file.

Command syntax

```
kesl-control [-T] --get-app-settings [--file <configuration file path>] [--json]
```

Arguments and keys

`--file <configuration file path>` – path to the configuration file where the application general settings will be displayed. 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. If the `--json` key is not specified, the settings will be imported in the INI format.

The kesl-control --set-app-settings command

This command configures the general application settings via command options or by importing settings from a configuration file.

Command syntax

Define settings via command options:

```
kesl-control [-T] --set-app-settings <option name>=<option value> [<option name>=<option value>]
```

Define settings via a configuration file:

```
kesl-control [-T] --set-app-settings --file <configuration file path> [--json]
```

Arguments and keys

`<option name>=<option value>`: the name and value of a general application setting.

`--file <configuration file path>` – full path to the configuration file from which you want to import settings into the application.

`--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` key 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.

Command syntax

```
kesl-control [-T] --get-settings <task ID/name> [--file <configuration file path>] [--json]
```

Arguments and keys

`<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.

`--file <configuration file path>` – path to the configuration file into which the task settings will be written. 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. If the `--json` key is not specified, the settings will be imported in the INI 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.

Command syntax

Define settings via command options:

```
kesl-control [-T] --set-settings <task name/ID> <option name>=<option value> [<option name>=<option value>] [--add-path <path>] [--del-path <path>] [--add-exclusion <path>] [--del-exclusion <path>]
```

Define settings via a configuration file:

```
kesl-control [-T] --set-settings <task name/ID> --file <configuration file path> [--json]
```

Arguments and keys

`<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.

`<setting name>=<setting value>` is the name and value of one of the task settings.

`--add-path <path>` adds the path to the directory with the objects to be scanned.

`--del-path <path>` deletes the path to the directory with the objects to be scanned.

`--add-exclusion <path>`: add the path to the directory with objects to exclude from scanning.

`--del-exclusion <path>` deletes the path to the directory with the objects to be excluded.

`--file <configuration file path>` – full path to the configuration file from which the task settings will be imported.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` key 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.

Command syntax

```
kesl-control [-T] --set-settings <task ID/name> --set-to-default
```

Arguments and keys

`< 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 kesl-control --get-schedule command

The command outputs the current schedule of the specified task to the console or a configuration file.

Command syntax

```
kesl-control [-T] --get-schedule < task ID/name > [--file < configuration file path >] [--
json]
```

Arguments and keys

`< 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.

`--file < path to configuration file >` is the path to the configuration file in which the settings for the task run schedule will be output. 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. If the `--json` key is not specified, the settings will be imported in the INI format.

The kesl-control --set-schedule command

The command defines a schedule for the specified task via command options or by importing settings from a configuration file.

Command syntax

Define settings via command options:

```
kesl-control [-T] --set-schedule < task ID/name > < option name >=< option value > [< option
name >=< option value >]
```

Define settings via a configuration file:

```
kesl-control [-T] --set-schedule < task ID/name > --file < configuration file path > [--
json]
```

Arguments and keys

`< 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.

`< setting name >=< setting value >` is the name and value of one of the settings for the task schedule.

`--file <configuration file path>` – full path to the configuration file from which the task schedule settings will be imported.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` key 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.

Command syntax

```
kesl-control [-T] --get-task-list [--json]
```

Arguments and keys

`--json` is specified to output the settings in JSON format.

kesl-control --get-task-state

This command outputs the status of the specified task.

Command syntax

```
kesl-control [-T] --get-task-state <task ID/name> [--json]
```

Arguments and keys

`<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.

`--json` is specified to output the settings in JSON format.

kesl-control --create-task

This command creates a task of the specified type with the default settings or settings specified in a configuration file.

Command syntax

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 the configuration file> [--json]
```

Arguments and keys

`< task name >` is the name that you specify for the new task.

`< task type >` is the identifier for the type of the created task.

`--file < configuration file path >`: the full path to the configuration file to import settings from.

`--json` is specified to import the settings from the configuration file in JSON format. If the `--json` key 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.

Command syntax

```
kesl-control [-T] --delete-task < task ID/name >
```

Arguments and keys

`< 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.

kesl-control --start-task

This command starts a task.

Command syntax

```
kesl-control [-T] --start-task < task ID/name > [-W] [--progress]
```

Arguments and keys

`< 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.

`[-W]`: enable current events output.

`[--progress]`: display task progress.

kesl-control --stop-task

This command stops a task.

Command syntax

```
kesl-control [-T] --stop-task < task ID/name > [-W]
```

Arguments and keys

< 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.

[-W]: enable current events output.

kesl-control --suspend-task

This command pauses a task.

Command syntax

```
kesl-control [-T] --suspend-task < task ID/name >
```

Arguments and keys

< 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.

kesl-control --resume-task

This command resumes a task.

Command syntax

```
kesl-control [-T] --resume-task < task ID/name >
```

Arguments and keys

< 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.

kesl-control --scan-file

This command creates and runs a custom scan task.

Command syntax

```
kesl-control [-T] --scan-file < path > [--action < action >]
```

Arguments and keys

< path >: the path to the file or directory to scan. You can specify multiple paths by separating them with a space.

--action < action > is the action to be performed by the application on the infected objects. If you do not specify the --action key, the application performs the recommended action.

kesl-control --scan-container

This command creates and runs a custom container or image scan task.

Command syntax

```
kesl-control [-T] --scan-container <container/image[:tag]>
```

Arguments and keys

`<container/image[:tag]>`: container/image ID/name You can use masks to scan several objects.

> 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.

The kesl-control --get-container-settings command

The command outputs the current general container scan settings to the console or a configuration file.

Command syntax

```
kesl-control [-C] --get-container-settings [--file <configuration file path>] [--json]
```

Arguments and keys

`--file <configuration file path>`: the path to the configuration file where general container scan settings will be saved 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. If the `--json` key is not specified, the settings will be imported in the INI format.

The kesl-control --set-container-settings command

The command configures the general container scan settings with command options or by importing settings from a configuration file.

Command syntax

Define settings via command options:

```
kesl-control [-C] --set-container-settings <setting name>=<setting value> [<setting name>=<setting value>]
```

Define settings via a configuration file:

```
kesl-control [-C] --set-container-settings --file <configuration file path> [--json]
```

Arguments and keys

`<option name> = <option value>`: the name and value of a general container scan setting.

`--file <configuration file path>`: the full path to the configuration file; general container scan settings from this file will be imported into the application.

`--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` key is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

Commands for managing encrypted connections scan settings

-N is a prefix indicating that the command belongs to the group of commands for managing secure connections 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.

Command syntax

```
kesl-control -N --query user

kesl-control -N --query auto

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.

Command syntax

```
kesl-control -N --clear-web-auto-excluded
```

kesl-control --get-net-settings

The command outputs the current encrypted connections scan settings to the console or a configuration file.

Command syntax

```
kesl-control [-N] --get-net-settings [--file <configuration file path>] [--json]
```

Arguments and keys

`--file <configuration file path>`: the path to the configuration file to output the encrypted connections scan settings to. 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. If the `--json` key is not specified, the settings will be imported in the INI format.

kesl-control --set-net-settings

The command configures the encrypted connections scan settings with command options or by importing settings from a configuration file.

Command syntax

Define settings via command options:

```
kesl-control [-N] --set-net-settings <option name>=<option value> [<option name>=
<option value>]
```

Define settings via a configuration file:

```
kesl-control [-N] --set-net-settings --file <configuration file path> [--json]
```

Arguments and keys

`<option name> = <option value>`: the name and value of an encrypted connections scan option.

`--file <configuration file path>`: the full path to the configuration file to import encrypted connections scan settings from.

`--json` is specified to import the settings from the configuration file into the application in JSON format. If the `--json` key is not specified, the application attempts to import from an INI file. If the import fails, an error is displayed.

kesl-control --add-certificate

This command adds a certificate to the list of trusted certificates.

Command syntax

```
kesl-control [-N] -add-certificate <path to certificate>
```

Arguments and keys

`< path to certificate >` is the path to the certificate file that you want to add (PEM or DER format).

kesl-control --remove-certificate

This command removes a certificate from the list of trusted certificates.

Command syntax

```
kesl-control [-N] --remove-certificate < certificate subject >
```

kesl-control --list-certificates

This command outputs a list of trusted certificates.

Command syntax

```
kesl-control [-N] --list-certificates
```

Statistics commands

-S is a prefix indicating that the command belongs to the statistics command group.

kesl-control --app-info

This command outputs information about the application.

Command syntax

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

Arguments and keys

`--json` is specified to output the settings in JSON format.

kesl-control --omsinfo

This command creates a JSON file for integration with Microsoft Operations Management Suite.

Command syntax

```
kesl-control [-S] --omsinfo --file < file name and path >
```

Commands for displaying events

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.

Command syntax

```
kesl-control -W [--query "<filter conditions>"]
```

Arguments and keys

<filter conditions>: one or several logical expressions in the format <field> <comparison operator> '<value>', combined with the logical operator and to output specific current events.

Commands for managing application events

-E: a prefix indicating 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.

Command syntax

```
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.

Command syntax

```
kesl-control -E --query "<filter conditions>" [--db <database file>] [-n <number>] --file <file name and path> [--json] [--reverse]
```

Arguments and keys

<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 global application setting.

<filter conditions>: one or several logical expressions in the format <field> <comparison operator> '<value>', combined with the help of the logical operator and to limit the results.

<number> – number of the latest events of the selection (number of records from the end of the selection) to be displayed.

`--file <file name and path>`: 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).

Commands for managing license keys

-L is a prefix indicating that the command belongs to the group of commands used to manage license keys.

Commands for adding and deleting license keys can be run only if the application is being used in standard mode. If Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments, commands for managing license keys finish with an error. You activate the application as part of Kaspersky Security for Virtualization Light Agent, and therefore do not need to activate the application separately.

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 an active application license key as well as an active EDR Optimum license key. You do not need to specify the type of the key in the command.

Command syntax

```
kesl-control [-L] --add-active-key <key file path>

kesl-control [-L] --add-active-key <activation code>
```

Arguments and keys

`<path to the key file>` – 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>` – activation code.

Example:
Add a key as an active key from the /home/test/00000001.key file:

```
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 an activation code.

You can use this command to add a reserve application license key as well as a reserve EDR Optimum license key. 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.

Command syntax

```
kesl-control [-L] --add-reserve-key <key file path>

kesl-control [-L] --add-reserve-key <activation code>
```

Arguments and keys

`<path to the key file>` – 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>` – activation code.

Example:
Add 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.

Command syntax

```
kesl-control [-L] --remove-active-key [--edr-optimum]
```

Arguments and keys

`--edr-optimum` – delete the active EDR Optimum license key. If you do not specify the `--edr-optimum` option, the active license key for Kaspersky Endpoint Security will be removed.

kesl-control --remove-reserve-key

This command lets you remove a reserve license key.

Command syntax

```
kesl-control [-L] --remove-reserve-key [--edr-optimum]
```

Arguments and keys

`--edr-optimum` – delete the reserve EDR Optimum license key. If you do not specify the `--edr-optimum` option, a reserve license key for Kaspersky Endpoint Security will be removed.

kesl-control -L --query

The `-L --query` command outputs information about the license that was used for activating the application and license keys currently in use.

Command syntax

```
kesl-control -L --query [--json]
```

Arguments and keys

`--json`: output data in JSON format.

kesl-control --load-mdr-blob

The `--load-mdr-blob` command downloads the BLOB configuration file required for integration with Kaspersky Managed Detection and Response.

Command syntax

```
kesl-control [-L] --load-mdr-blob <path to MDR BLOB configuration file>
```

kesl-control --remove-mdr-blob

The `--remove-mdr-blob` command removes the BLOB configuration file required for integration with Kaspersky Managed Detection and Response.

Command syntax

```
kesl-control [-L] --remove-mdr-blob
```

Commands for Firewall Management

-F: a prefix indicating that the command belongs to the firewall management commands.

kesl-control --add-rule

This command adds a new network packet rule.

Command syntax

```
kesl-control [-F] --add-rule [--name <rule name>] [--action <action>] [--protocol
<protocol>] [--direction <direction>] [--remote <remote address>[:<port range>]] [--
local <local address>[:<port range>]] [--at <index>]
```

Arguments and keys

`--name <rule name>` is the name of the network packet rule.

`--action <action>` is the action to be performed on connections specified in network packet rule.

`--protocol <protocol>` is the type of data transfer protocol for which you want to monitor network activity.

`--direction <direction>` is the direction of the monitored network activity.

`--remote <remote address>[:<port range>]`: the network address of the remote device.

`--local <local address>[:<port range>]`: the network address of the device with Kaspersky Endpoint Security installed.

`--at <index>`: the number of the rule in the list of network packet rules. If the `--at` key 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.

Command syntax

```
kesl-control -F --del-rule --name <rule name>

kesl-control [-F] --del-rule --index <index>
```

Arguments and keys

`--name <rule name>` is the name of the network packet rule.

`--index <index>`: 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.

Command syntax

```
kesl-control [-F] --move-rule --name <rule name> --at <index>

kesl-control [-F] --move-rule --index <index> --at <index>
```

Arguments and keys

`--name <rule name>` is the name of the network packet rule.

`--index <index>`: the current number of the rule in the list of network packet rules.

`--at <index>`: 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.

Command syntax

```
kesl-control [-F] --add-zone --zone <zone> --address <address>
```

Arguments and keys

`--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.

Command syntax

```
kesl-control [-F] --del-zone --zone <zone> --address <address>
```

```
kesl-control [-F] --del-zone --zone <zone> --index <address index>
```

Arguments and keys

`--zone <zone>` is the predefined name of the network zone.

`--address <address>` is the network address or subnet.

`--index <address index>`: the number of the address in the network zone.

kesl-control -F --query

This command displays firewall rules created with Kaspersky Endpoint Security.

Command syntax

```
kesl-control -F --query
```

Commands used to manage blocked devices

-H is a prefix indicating that the command belongs to the group of commands for managing devices blocked by Anti-Cryptor and Network Threat Protection.

The kesl-control --get-blocked-hosts command

The command allows you to output the list of blocked devices to the console.

Command syntax

```
kesl-control [-H] --get-blocked-hosts
```

The kesl-control --allow-hosts command

The command allows you to unblock blocked devices.

Command syntax

```
kesl-control [-H] --allow-hosts <address>
```

Arguments and keys

<address> is an IP address of the 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 managing Device Control

-D is a prefix indicating that the command belongs to the group of commands to manage Device Control.

kesl-control --get-device-list

The command outputs to the console a list of devices that are installed on a client device or connected to it.

Command syntax

```
kesl-control [-D] --get-device-list [--json]
```

Arguments and keys

`--json`: output data in JSON format.

Commands for managing Application Control

-A is a prefix indicating that the command belongs to the group of commands to manage Application Control.

kesl-control --get-app-list

The command outputs a list of applications found on a client device by the Inventory task.

Command syntax

```
kesl-control [-A] --get-app-list [--json]
```

Arguments and keys

`--json`: output data in JSON format.

kesl-control --get-categories

This command outputs a list of created application control categories.

Command syntax

```
kesl-control [-A] --get-categories [--names <name of category 1> <name of category 2> ... <name of category N>] [--file <path to configuration file>] [--json]
```

Arguments and keys

`<name of category 1> <name of category 2> ... <name of category N>` – names of the categories whose information you want to view. If you want to view information about several categories, specify the names of the categories, separated by a space.

`--file <path to configuration file>` – full path to the JSON configuration file to which the settings will be output.

`--json`: output data in JSON format.

kesl-control --set-categories

This command lets you create or edit the list of created Application Control categories.

Command syntax

```
kesl-control [-A] --set-categories [--names <name of category 1> <name of category 2> ... <name of category N>] --file <path to configuration file>
```

Arguments and keys

`<name of category 1> <name of category 2> ... <name of category N>` – names of the categories whose information you want to change. 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, the category will be removed from the list.

`--file <path to configuration file>` – full path to the configuration file with the category settings.

kesl-control --get-settings

This command outputs a list of created application control rules.

Command syntax

```
kesl-control --get-settings 21 [--file <path to configuration file>] [--json]
```

Arguments and keys

`--file <path to configuration file>` – full path to the configuration file to which the settings will be exported.

`--json`: output data in JSON format.

kesl-control --set-settings

This command lets you edit the list of created application categories and Application Control rules.

Command syntax

```
kesl-control --set-settings 21 [--file <path to configuration file>] [--json]
```

Arguments and keys

`--file <path to configuration file>` – full path to the configuration file from which the settings will be imported.

`--json` – import data from a JSON file.

kesl-control --set-to-default

This command lets you delete a list of application categories and Application Control rules.

Command syntax

```
kesl-control --set-settings 21 --set-to-default
```

Web Control management commands

kesl-control --get-settings

This command lets you display the list of specified Web Control settings.

Command syntax

```
kesl-control --get-settings 26 [--file <path to configuration file>] [--json]
```

Arguments and keys

`--file <path to configuration file>` – full path to the configuration file to which the settings will be exported.

`--json`: output data in JSON format.

kesl-control --set-settings

This command lets you edit the list of specified Web Control settings.

Command syntax

```
kesl-control --set-settings 26 [--file <path to configuration file>] [--json]
```

Arguments and keys

`--file <path to configuration file>` – full path to the configuration file from which the settings will be imported.

`--json` – import data from a JSON file.

kesl-control --set-to-default

This command lets you delete specified settings and reset Web Control settings to the default rule.

Command syntax

```
kesl-control --set-settings 26 --set-to-default
```

Commands for managing Backup

-B is a prefix indicating that the command belongs to the group of commands used to manage the Backup storage.

kesl-control --mass-remove

The command deletes some or all objects from Backup.

Command syntax

Delete all objects:

```
kesl-control [-B] --mass-remove
```

Delete objects that match the filter conditions:

```
kesl-control [-B] --mass-remove --query "<filter conditions>"
```

Arguments and keys

`<filter conditions>`: one or several logical expressions in the format `<field> <comparison operator> '<value>'`, combined with the help of the logical operator `and` to limit the results.

kesl-control -B --query

This command outputs information about Backup objects.

Command syntax

Output information about all objects in Backup:

```
kesl-control -B --query [-n <number>] [--json] [--reverse]
```

Output information about Backup objects that match the filter conditions:

```
kesl-control -B --query ["<filter conditions>"] [-n <number>] [--json] [--reverse]
```

Arguments and keys

`<filter conditions>`: one or several logical expressions in the format `<field> <comparison operator> '<value>'`, combined with the help of the logical operator `and` to limit the results. If you do not specify any filter conditions, the application will display the details of all objects in Backup.

< number >: the number of the most recent objects to display. If you do not specify the -n switch, the last 30 objects will be displayed. Specify 0 to show all objects.

--json: output data in JSON format.

kesl-control --restore

This command restores an object from Backup.

Command syntax

```
kesl-control [-B] --restore < object ID > [--file < file name and path >]
```

Arguments and keys

< object ID >: the ID of the Backup object.

--file < file name and path >: 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 object will be restored with its original name and to its original location.

Commands for managing users and roles

-U is a prefix indicating that the command belongs to the group of commands for managing users and roles.

kesl-control --get-user-list

This command outputs a list of users and roles.

Command syntax

```
kesl-control [-U] --get-user-list
```

kesl-control --grant-role

This command assigns a role to a specific user.

Command syntax

```
kesl-control [-U] --grant-role < role > < user >
```

kesl-control --revoke-role

This command revokes a role from a specific user.

Command syntax

```
kesl-control [-U] --revoke-role < role > < user >
```

Commands for managing settings for Kaspersky Endpoint Detection and Response (KATA) Integration

-R is a prefix indicating that the command belongs to the group of commands for managing the settings of integration with Kaspersky Endpoint Detection and Response (KATA) and Kaspersky Endpoint Detection and Response Optimum.

kesl-control --add-kataedr-server-certificate

This command adds or replaces a previously added KATA server certificate.

Command syntax

```
kesl-control [-R] --add-kataedr-server-certificate <file name and path>
```

Arguments and keys

`<file name and path>` are the name and path to the file containing the server certificate.

kesl-control --remove-kataedr-server-certificate

This command deletes a KATA server certificate.

Command syntax

```
kesl-control [-R] --remove-kataedr-server-certificate
```

kesl-control --query-kataedr-server-certificate

This command outputs information about a KATA server certificate.

Command syntax

```
kesl-control [-R] --query-kataedr-server-certificate
```

kesl-control --add-kataedr-client-certificate

This command adds or replaces a previously added client certificate used to secure the connection to a KATA server.

Command syntax

```
kesl-control [-R] --add-kataedr-client-certificate <file name and path>
```

Arguments and keys

`<file name and path>` is the name and path to the cryptocontainer (PFX archive) containing the client certificate and private key.

kesl-control --remove-kataedr-client-certificate

This command deletes the client certificate used to secure the connection to a KATA server.

Command syntax

```
kesl-control [-R] --remove-kataedr-client-certificate
```

kesl-control --query-kataedr-client-certificate

The command outputs information about a client certificate.

Command syntax

```
kesl-control [-R] --query-kataedr-client-certificate
```

kesl-control --isolation-stat

This command outputs the current state of network isolation to the console: enabled or disabled.

Command syntax

```
kesl-control [-R] --isolation-stat
```

kesl-control --isolation-off

This command lets you disable network isolation of a device.

Command syntax

```
kesl-control [-R] --isolation-off
```

Application commands in Light Agent mode for protecting virtual environments

-V: a prefix indicating that the command belongs to the group of Kaspersky Endpoint Security commands used in Light Agent mode for protecting virtual environments (as part of Kaspersky Security for Virtualization Light Agent).

> The commands can be executed only if Kaspersky Endpoint Security is used in Light Agent mode to protect virtual environments.

kesl-control --ksvla-info

This command outputs information about using the application in Light Agent mode for protecting virtual environments:

Command syntax

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

kesl-control --viis-info

This command outputs information about the connection of Light Agent (Kaspersky Endpoint Security used as a Light Agent as part of Kaspersky Security for Virtualization Light Agent) to the Integration Server:

Command syntax

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

kesl-control --svm-info

This command outputs information about the connection of Light Agent (Kaspersky Endpoint Security used as a Light Agent as part of Kaspersky Security for Virtualization Light Agent) to an SVM:

Command syntax

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

Appendix 3. 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:
  - autoinstall.ini configuration file, used when installing the application via Kaspersky Security Center.
  - Configuration file used when installing the application via the command line.
- 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 application 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 [ ].
- Enter the values of settings in the format < `setting name` >=< `setting value` > (spaces between the a 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.

Preset configuration files

After the initial setup, 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 these files.

The default values in these files should be changed only under the supervision of Technical Support specialists and in accordance with their instructions.

Settings of the kesl.ini configuration file

Setting	Description	Values
The **[General]** section contains the following settings:		
`Locale`	The locale used for the localization of texts sent by Kaspersky Endpoint Security to Kaspersky Security Center (events, notifications, task results, etc.). The locale of the graphical interface and the application command line depends on the value of the `LANG` environment variable. If the locale that is not supported by Kaspersky Endpoint Security is specified as the value of the `LANG` environment variable, the graphical interface and the command line are displayed in English.	The locale in the format spe If the `Locale` setting is not operating system locale is u application fails to determi system localization languag system localization is not su value will be used – `en_US`.
`PackageType`	Format of the installed application package. This setting does not affect the operation of the application. The value of the setting is filled in automatically during initial application configuration.	`rpm` – an RPM package is in `deb` – a DEB package is ins
`UseFanotify`	Indicates use of fanotify notifications. This setting does not affect the operation of the application. The value of the setting is filled in automatically during initial application configuration.	`true/yes` – The operating fanotify notifications. `false/no` – The operating support fanotify notificatic
`KsvlaMode`	Kaspersky Endpoint Security usage mode. This setting does not affect the operation of the application. The value of the setting is filled in automatically during initial application configuration.	`true/yes` – the applicatio Agent mode to protect virt `false/no` – the applicatio mode.
`StartupTraces`	Enables generation of trace files at application startup.	`true/yes` – Create trace f startup. `false/no` (default value) – files at application startup.
`RevealSensitiveInfoInTraces`	Display information in trace files that may contain personal data (for example, passwords).	`true/yes` (default value) – in application trace files tha personal data. `false/no` (default value) – information that may conta trace files.
`AsyncTraces`	Enables asynchronous tracing, in which information is logged to trace files in asynchronously.	`true/yes` – enable asynch `false/no` (default value) – asynchronous tracing.

`CoreDumps`	Enables the creation of a dump file when application failure occurs.	`true/yes` – Create a dump application crashes. `false/no` (default value) – dump file when the applicat
`CoreDumpsPath`	Path to the directory where the dump files are stored.	Default value: /var/opt/kaspersky/kesl/co Root privileges are required default dump file directory.
`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 memory in megabytes.	Default value: 8192.
`MachineId`	The user's unique device ID.	The value of the setting is f during installation of the ap
`SocketPath`	Path to a socket for a remote connection to, say, a graphical interface and the kesl-control utility.	Default value: /var/run/bl4c
`MaxInotifyWatches`	Limit on the number of subscriptions to changes in files and directories (user watches) in /proc/sys/fs/inotify/max_user_watches.	Default value: 300000.
`MaxInotifyInstances`	Limit on the number of subscriptions to changes in files and directories for a single user.	Default value: 2048.
`ExecEnvMax`	The number of environment variables that the application captures from the command call.	Default value: 50.
`ExecArgMax`	Number of arguments that the application captures from the exec call.	Default value: 50.
`DisableFileAvActions`	Disables the disinfection and file deletion functions for application components after its installation. If the disinfection and file deletion functions are disabled and a threat is detected, the application does not attempt to disinfect or delete the files in which a threat was detected, but only informs the user about a threat detection.	`true/yes`: disables the dis deletion functions when th started after the installatio `false/no` (default value): d disinfection and file deletio application is started after
`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: • Google Public DNS™ (8.8.8.8).	`true/yes` – Use a public D Kaspersky servers. `false/no` (default value) – DNS to access Kaspersky s

	• Cloudflare® DNS (1.1.1.1). • Alibaba Cloud® DNS (223.6.6.6). • Quad9® DNS (9.9.9.9). • CleanBrowsing (185.228.168.168).	The application's request domain addresses and th address, since the applic TCP/UDP connection wit This information is neces to check the certificate when interacting via HTT application is using a pub data processing rules are Privacy Policy of the corr If you need to block the a using a public DNS serve Technical Support for a p
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 hexadec prefix 0x. Default value: 0x100.
`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 hexadec prefix 0x. Default value: 0x200.
`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 hexadec prefix 0x. Default value: 0x400.
`BypassNFlogMark`	A mark used to indicate packages created or scanned by the application to prevent them from being logged by the iptable utility.	A decimal value or hexadec prefix 0x. Default value: 0x800.
`ProxyRouteTable`	Number of the routing table.	Default value: 101.
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 to protect virtual environments: server or workstation. This setting does not affect the operation of the application. The value of the setting is filled in automatically during initial application configuration.	`true/yes` – the protected used as a server. `false/no` – the protected used as a workstation.
`VdiMode`	Enables VDI protection mode when using	`true/yes` – VDI protectio

	the application in Light Agent mode to protect virtual environments. This setting does not affect the operation of the application. The value of the setting is filled in automatically during initial application configuration.	`false/no` – VDI protectio
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`	Maximum time to wait for the application to start (in minutes), after which the kesl process will be restarted.	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 a server in response to a received PING message.	Default value: 2000 ms.
`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 terminate the kesl process.	Default value: 2 minutes.
`ConnectTimeout`	Maximum time from the start of the kesl process to the moment when a connection with the Watchdog server is established by the application. If the application does not establish a connection in this time interval, the Watchdog server begins the procedure to terminate 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 ms.
`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.

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 terminate the kesl process.	off – the resident set size < value >% – a value betwe expressing a percentage of < value >MB – a value in me lowest/< value >%/< val value between the value as the value in megabytes. highest/< value >%/< va value between the value as the value in megabytes. auto – up to 50% of availa less than 2GB and not more 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 terminate the kesl process.	off (default value) – The v not limited. < value >MB – a value in me
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 terminate the kesl process.	off (default value) – The s not limited. < value >% – a value betw expressing a percentage of < value >MB – a value in me lowest/< value >%/< val value between the value as the value in megabytes. highest/< value >%/< va value between the value as the value in megabytes.
TrackProductCrashes	Enabling application stability monitoring. If application stability monitoring is enabled, the Watchdog server tracks the number of abnormal halts of the application.	true/yes – enable applica monitoring. false/no (default value) – stability monitoring.
ProductHealthLogFile	The path to the file used for application stability monitoring.	Default value: /var/opt/kaspersky/kesl/pr
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 seconc
WarnAfter_#_crash	Number of abnormal halts of the application that are required before displaying a notification about unstable application operation.	Default value: 10. If the value is 0, an unstable notification is not displayed
WarnRemovingThreshold	Time interval (in seconds) after which the application's unstable status will be cleared.	Default value: 86400 secor

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.	`true/yes` – enable suppor environment in the operatic Monitoring component. `false/no` – do not enable containerd environment in t Container Monitoring comp

Default command line task settings

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 File_Threat_Protection task (ID:1)

```
ScanArchived=No

ScanSfxArchived=No

ScanMailBases=No

ScanPlainMail=No

SkipPlainTextFiles=No

TimeLimit=60

SizeLimit=0

FirstAction=Recommended

SecondAction=Block

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 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

FirstAction=Recommended

SecondAction=Skip

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 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

FirstAction=Recommended

SecondAction=Skip

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 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

FirstAction=Recommended

SecondAction=Skip
```

```
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 Update task (ID:6)

```
SourceType="KLServers"

UseKLServersWhenUnavailable=Yes

ApplicationUpdateMode=DownloadOnly

ConnectionTimeout=10
```

Default settings for Backup task (ID:10)

```
DaysToLive=90

BackupSizeLimit=0

BackupFolder=/var/opt/kaspersky/kesl/common/objects-backup/
```

Default settings for 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 Firewall_Management task (ID:12)

```
DefaultIncomingAction=Allow

DefaultIncomingPacketAction=Allow

OpenNagentPorts=Yes

[NetworkZonesTrusted]

[NetworkZonesLocal]

[NetworkZonesPublic]
```

Default settings for 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 Web_Threat_Protection task (ID:14)

```
UseTrustedAddresses=Yes

ActionOnDetect=Block

CheckMalicious=Yes

CheckPhishing=Yes

UseHeuristicForPhishing=Yes

CheckAdware=No

CheckOther=No
```

Default settings for Device_Control task (ID:15)

```
OperationMode=Block

[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 Removable_Drives_Scan task (ID:16)

```
ScanRemovableDrives=NoScan

ScanOpticalDrives=NoScan

BlockDuringScan=No
```

Default settings for 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

FirstAction=Recommended

SecondAction=Skip

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
```

You can also use the option in this configuration file for the Custom Container Scan task.

Default settings for Behavior_Detection task (ID:20)

```
UseTrustedPrograms=No

TaskMode=Block
```

Default settings for Application_Control task (ID:21)

```
AppControlMode=DenyList

AppControlRulesAction=ApplyRules
```

Default settings for Inventory_Scan task (ID:22)

```
ScanScripts=Yes

ScanBinaries=Yes

ScanAllExecutable=Yes

CreateGoldenImage=No
```

```
[ScanScope.item_0000]

AreaDesc=All objects

UseScanArea=Yes

Path=/usr/bin

AreaMask.item_0000=*
```

Default settings for KATAEDR task (ID:24)

```
UseClientPinnedCertificate=No

SynchronizationPeriod=5

ConnectionTimeout=10

RequestTimeout=10

EnableTelemetry=Yes

[Endpoints.item_0000]

Address=

Port=443

[EventTransferSettings]

MaximumDataTransferTime=30

UseRequestCountLimits=Yes

MaximumNumberOfEventsInHour=3000

EventLimitExceededPercentage=15
```

Default settings for Web_Control task (ID:26)

```
WebControlDefaultAction=Allow

ComplaintRecipient=
```

General application settings

General application settings define 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 standard directory of the S configuration file on the compu by default. Default value: /etc/samba/smb The application must be restar is changed.
`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 standard directory of the I file on the computer is specifie Default value: /etc/exports. The application must be restar is changed.
`TraceLevel`	Enable application tracing and the level of detail in the trace files.	`Detailed` – Generate a detail `MediumDetailed` – Generate contains informational messag messages. `NotDetailed` – Generate a tr error messages. `None` (default value) — Do not
`TraceFolder`	The directory that stores the application trace files.	Default value: /var/log/kaspers If you specify a different direct the account under which Kasp Security is running has read/wr for this directory. Root privileg access the default trace files c The application must be restar is changed.
`TraceMaxFileCount`	Maximum number of application trace files.	1–10000 Default value: 10. The application must be restar is changed.
`TraceMaxFileSize`	Specifies the maximum size of an application trace file (in megabytes).	1–1000 Default value: 500. The application must be restar is changed.
`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 is not available for operating systems that use the fanotify technology.	4096–33554432 Default value: 16384. After changing the value of thi Threat Protection task needs t
`DetectOtherObjects`	Enable detection of legitimate applications that intruders can	`Yes`: enable detection of legiti that intruders can use to comp

	use to compromise devices or data.	data. `No` (default): disable detection applications that intruders can 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) — Enable s namespaces and containers. `No` — Disable scanning of name containers.
`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.	`Yes` (default value) to block ac duration of the scan. `No` to allow access to files duri Requests to any file is allowed, asynchronously. This file opera mode has less impact on the s but there is a risk that a threat disinfected or deleted if the fil change its name during a scan application makes a decision o file.
`UseKSN`	Enabling Kaspersky Security Network usage:	`Basic` - enable use of Kaspers in standard mode. `Extended` - enable use of Kas Network in extended mode. `No` (default value) — disable us Security Network.
`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` — enable the operating m Kaspersky Endpoint Security u version of the malware databa `No` (default value) – use the fu malware databases. Cloud mode is disabled auto KSN is disabled.
`UseMDR`	Enabling the Managed Detection and Response component for integration with Kaspersky Managed Detection and Response.	`Yes` to enable the Managed De Response component. `No` (default value) – disable the and Response component.
`UseProxy`	Enables use of a proxy server by Kaspersky Endpoint Security	`Yes` - enable the use of a prox

	components. A proxy server can be used to communicate with Kaspersky Security Network and Kaspersky Endpoint Detection and Response (KATA) to activate the application, and when updating application databases and modules. 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.	`No` (default) - Disable the use c If `Yes` is selected, integration v Endpoint Detection and Respc through a proxy server.
`ProxyServer`	Proxy server options in the format: `[<user>[:<password>]@]<proxy server address>[:<port>]`. 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.	—
`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 0 is specified, events are not
`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 can start.	0–4294967295 Default value: 0. If 0 is specified, a non-privilege custom scan tasks. If you installed the graphical us when installing the application, `LimitNumberOfScanFileTas` default value `5`.
`UseSyslog`	Enable logging of information about events to syslog Root privileges are required to access syslog.	`Yes` — Enable logging of inform to syslog. `No` (default value) — Disable lo about events to syslog.

`EventsStoragePath`	The database directory where the application saves information about events. Root privileges are required to access the default event database.	Default value: /var/opt/kaspersky/kesl/privat
`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` — Exclud directories mounted on the de NFS protocols from file operat `Mounted:NFS` — Exclude all re mounted on the device using t from file operation interceptio `Mounted:SMB` — Exclude all re mounted on the device using t from file operation interceptio `Mounted:<file system ty` mounted directories with the s type from file operation interc `/mnt` — Exclude objects in the (including subdirectories) from interception. This directory is u temporary mount point for ren `<path that contains the /mnt/**/user_share>` — Exc mount points whose names co mask from file operation interc

		You can use the * (asterisk) create a file or directory nam You can indicate a single * c represent any set of charact empty set) preceding the / file or directory name. For ex /dir/*/file or /dir/*/* You can indicate two consec to represent any set of char an empty set and the / char directory name. For example /dir/**/file*/ or /dir/ The ** mask can be used or directory name. For example /dir/**/**/file is an inc To exclude the mount point specifically indicate /dir (n The mask /dir/* excludes the level below /dir but not /dir/** mask excludes all n the level of /dir but not /d You can use a single ? chara any one character in the file
MemScanExcludedProgramPath.item_#	Exclude process memory from scans. The application does not scan the memory of the indicated process.	< full path to process > - process in the indicated local c masks to specify the path.

		You can use the * (asterisk) create a file or directory nam You can indicate a single * c represent any set of charact empty set) preceding the / file or directory name. For ex /dir/*/file or /dir/*/* You can indicate two consec to represent any set of char an empty set and the / char directory name. For example /dir/**/file*/ or /dir/ The ** mask can be used or directory name. For example /dir/**/**/file is an inc You can use a single ? chara any one character in the file
UseOnDemandCPULimit	Enables CPU usage limits for the *ODS*, *ContainerScan*, and *InventoryScan*-type tasks.	Yes: enable the CPU usage lim *ContainerScan*, and *Inventory* No (default): disable CPU usag
OnDemandCPULimit	The maximum utilization of all processor cores (as a percentage) when running *ODS*, *ContainerScan*, and *InventoryScan*-type tasks.	10–100 Default value: 100.
UseEdrOptimum	Enabling the EDR Optimum component for integration with Kaspersky Endpoint Detection and Response Optimum.	Yes – Enable the EDR Optimu No (default) – Disable the EDR component.

General Container Scan settings

The container scan general settings 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.	StopContainerIfFailed (default value) — Stop the container if an infected object cannot be disinfected or deleted. StopContainer — Stop the container when an infected object is detected.

	File Threat Protection task settings are used when scanning objects inside a container. The action performed on a container when an infected object is detected also depends on the File Threat Protection task settings (see the table below).	`Skip` — Do not perform any action on containers when an infected object is detected.
`UseDocker`	Use the Docker environment.	`Yes` (default value) — Use the Docker environment. `No` — Do not use the Docker environment.
`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.

The action to be performed on the container upon detection of an infected object may vary depending on the specified values of the `FirstAction` and `SecondAction` parameters of the File Threat Protection task.

Relationship between actions performed on containers and the specified action performed on infected objects

Value of the FirstAction / SecondAction setting	Action performed on the container when the StopContainerIfFailed action is selected
`Disinfect`	Stop the container if disinfection of an infected object fails.
`Remove`	Stop the container if an infected object removal fails.

Encrypted connections scan settings

Setting	Description	Values
`EncryptedConnectionsScan`	Enables or disables encrypted traffic scan. For the FTP protocol, secure connections scan is disabled by default.	`Yes` (default value)—Enable secure connection scans. `No`: disable encrypted connection scanning. The application does not decrypt the encrypted traffic.
`EncryptedConnectionsScanErrorAction`	Specifies the action to perform when a secure 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.
`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.

The **[Exclusions.item_#]** section contains domains excluded from scans. The application does not scan secure connections established when visiting specified domains.		
`DomainName`	Specifies the domain name. You can use masks to specify the domain.	The default value is not defined.
The **[NetworkPorts.item_#]** section contains the network ports monitored by the application.		
`PortName`	Network port description.	The default value is not defined.
`Port`	Network port numbers to be monitored by the application.	`1 – 65535` The default value is not defined.

Tasks schedule settings

Task start schedule settings

Setting	Description	Values
`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 `StartTime` option is required if the `RuleType` option is set to one of the following: Once, Monthly, Weekly, Daily, Hourly, or Minutely.	`[< year >/< month >/< day of the month >] [ hh ]:[ mm ]:[ ss ]; [< day of the month >|< day of the week >]; [< start periodicity >]`.
`RandomInterval`	A time interval from 0 to the specified value (in minutes), which will be added to the task start time to avoid starting tasks at the same time.	
`RunMissedStartRules`	Run a missed task after the	`Yes`: enables running a missed task after

	application starts.	the application starts. `No`: does not enable running a missed task after the application starts.

Appendix 4. Command line return codes

Kaspersky Endpoint Security has the following command line return codes:

0 – command/task completed successfully.

1 – general error in command arguments.

2 – error in passed application settings.

64 – Kaspersky Endpoint Security is not running.

66 – application databases are not downloaded (used only by the `kesl-control --app-info` command).

67 – activation 2.0 ended with an error due to network problems.

68 – the command cannot be executed because the application is running under a policy.

69 – the application is located in the Amazon Paid Ami infrastructure.

70 – an attempt to start a running task, 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 – an attempt to specify the Application Control task settings that affect the application operation without confirming these settings using the `--accept` flag.

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.

128 – unknown error.

65 – all other errors.

Appendix 5. 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>
   ```

Sources of information about Kaspersky Endpoint Security

Kaspersky Endpoint Security page in the Knowledge Base

The *Knowledge Base* is a section of the Kaspersky Technical Support website.

On the Kaspersky Endpoint Security page in the Knowledge Base, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use the application.

Articles in the Knowledge Base may provide answers to questions that relate both to Kaspersky Endpoint Security as well as to other Kaspersky applications. Articles in the Knowledge Base may also contain Technical Support news.

Discuss Kaspersky applications on the forum

If your question does not require an immediate answer, you can discuss it with Kaspersky experts and other users on the Forum.

The Forum lets you view discussion topics, post comments, and create new discussion topics.

Glossary

Active key

A key that is currently used by the application.

Active policy

Policy currently used by the application to control data leaks. The application can use several policies at the same time.

Administration group

A set of devices combined in Kaspersky Security Center in accordance with the functions they perform and the set of Kaspersky applications installed on them. Devices are grouped to simplify administration as the group of devices can be managed as a single entity. An administration group can include other groups. For each application installed in the administration group, group policies and group tasks can be created.

Administration Server

A component of Kaspersky Security Center that centrally stores information about all Kaspersky applications installed within the corporate network. It can also be used to manage these applications.

Application activation

Switching the application to the fully functional mode. Application activation is performed during or after the installation of the application. You need an activation code or a key file to activate the application.

Application databases

Databases that contain information about computer security threats known to Kaspersky as of when the databases are released. Application databases are created by Kaspersky experts and updated hourly.

Application settings

Application settings that are common to all types of tasks and govern the overall operation of the application, such as application performance settings, reporting settings, and backup settings.

Database of malicious web addresses

A list of web resources whose content may be considered as dangerous. The list is created by Kaspersky experts; it is regularly updated and is included in the distribution kit of Kaspersky applications.

Database of phishing web addresses

A list of web resource addresses that are identified by Kaspersky experts as phishing. The database is regularly updated and is included in the distribution kit of Kaspersky applications.

Exclusion

Exclusion is an object excluded from the Kaspersky application scan. You can exclude from scan files of certain formats, file masks, a certain area (for example, a folder or an application), application processes, or objects by name, according to the Virus Encyclopedia classification. Each task can be assigned a set of exclusions.

False positive

A situation when a Kaspersky application considers a non-infected object to be infected because the object's code is similar to that of a virus.

File mask

Representation of a file name using wildcards. The standard wildcards used in file masks are * and ?, where * is any number of any characters, and ? is any single character.

Group policy

see Policy.

Group task

A task assigned to an administration group and performed on all managed devices included in this administration group.

Infected object

An object which includes a portion of code that completely matches the part of a known malware code. Kaspersky experts do not recommend accessing such objects.

Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent component. Interacts between Kaspersky Endpoint Security components and the virtual infrastructure.

Kaspersky update servers

Kaspersky HTTP and FTP servers from which Kaspersky applications download database and application module updates.

License

A time-limited right to use the application, granted under the End User License Agreement.

License certificate

A document that you receive from Kaspersky along with the key file or activation code. This document contains information about the license provided.

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent component. Installed on each virtual machine that needs to be protected.

Object disinfection

A method of processing infected objects that results in full or partial recovery of data. Not all infected objects can be disinfected.

Policy

A policy determines the application settings and manages the access to configuration of an application installed on devices within an administration group. An individual policy must be created for each application. You can create an unlimited number of various policies for applications installed on the devices in each administration group, but only one policy can be applied to each application at a time within an administration group.

Proxy server

A computer network service which allows users to make indirect requests to other network services. First, a user connects to a proxy server and requests a resource (e.g., a file) located on another server. Then the proxy server either connects to the specified server and obtains the resource from it or returns the resource from its own cache (if the proxy has its own cache). In some cases, a user's request or a server's response can be modified by the proxy server for certain purposes.

Reserve key

A key that certifies the right to use the application but is not currently being used.

SIEM system

A *SIEM (Security Information and Event Management)* system is a solution for managing information and events withing the security system of an organization.

Startup objects

A set of applications needed for the operating system and software that is installed on the computer to start and operate correctly. These objects are executed every time the operating system is started. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

Subscription

Enables use of the application with the selected settings (expiration date and the number of devices). You can pause or resume your subscription, renew it automatically, or cancel it.

SVM

Secure virtual machine – a special virtual machine on which the scanserver service (Protection Server, a component of Kaspersky Endpoint Security for Virtualization Light Agent) is installed.

Trusted device

Device that can be fully accessed at any time by the users listed under the trusted device settings.

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.

Amazon is a trademark of Amazon.com, Inc. or its affiliates.

FireWire is a trademark of Apple Inc.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

The Bluetooth word, mark and logos are owned by Bluetooth SIG, Inc.

Ubuntu and LTS are registered trademarks of Canonical Ltd.

Citrix, XenServer are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in 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.

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, Google Public DNS are trademarks of Google LLC.

HUAWEI, EulerOS, and FusionSphere are trademarks of Huawei Technologies Co., Ltd.

Intel, Core are trademarks of Intel Corporation in the U.S. and/or other countries.

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

Microsoft, Active Directory, Hyper-V, Outlook, Visual C++, and Windows 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 and JavaScript are registered trademarks of Oracle and/or its affiliates.

Red Hat, Red Hat Enterprise Linux, and CentOS are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Debian is a registered trademark of Software in the Public Interest, Inc.

SUSE is a registered trademark of SUSE LLC in the United States and other countries.

VMware, VMware NSX, VMware NSX Manager, VMware Tools, VMware vCenter, VMware vSphere are trademarks of VMware, Inc. or registered trademarks of VMware, Inc in the United States and other jurisdictions.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.