



Kaspersky Endpoint Security 10 for Windows

User Manual

Document version: 1.03

Application version: 10.3.0.6294 AES256

Table of Contents

About Kaspersky Endpoint Security 10 for Windows	5
Distribution kit	5
Hardware and software requirements	6
Environment and operation requirements	8
User and administrator roles in the application	9
License and activation	10
Managing the application on a client computer	11
Application functions in the Windows context menu	11
Application icon context menu	13
Web Control	14
About Web Control	14
Web Control subsection	30
Application Privilege Control	46
About Application Privilege Control	46
Application Privilege Control subsection	47
Application Startup Control	84
About Application Startup Control	84
Application Startup Control subsection	84
Device Control	112
About Device Control	112
Device Control subsection	113
Anti-Virus protection	134
Anti-Virus protection section	136
Protecting the computer file system. File Anti-Virus	155
Email protection. Mail Anti-Virus	173
Computer protection on the Internet. Web Anti-Virus	184
Protection of IM client traffic. IM Anti-Virus	191
System Watcher	194
Scanning the computer	199
Managing Quarantine and Backup	243
About Quarantine and Backup	244
Configuring Quarantine and Backup settings	245
Managing Quarantine	247

Managing Backup.....	252
Working with encrypted devices when there is no access to them	255
Obtaining access to encrypted devices through the application interface	257
Creating the executable file of Restore Utility.....	258
Restoring data on encrypted devices using the Restore Utility.....	259
Using Authentication Agent.....	262
Main window of Authentication Agent.....	262
Restoring Authentication Agent account credentials	263
Step 1. Entropy.....	264
Step 2. Challenge.....	264
Step 3. Response.....	264
Remote administration of the application through Kaspersky Security Center.....	265
About managing the application via Kaspersky Security Center.....	265
Managing policies.....	266
About policies.....	267
Application Startup Control.....	271
Application Privilege Control.....	283
Device Control.....	319
Web Control	344
Data Encryption.....	376
Anti-Virus protection	401
Advanced application settings.....	467
Tasks.....	489
About tasks for Kaspersky Endpoint Security.....	489
Key addition task settings section	491
Application components modification task settings section	493
Authentication Agent account management task settings section.....	495
Settings section	496
Managing the application from the command prompt.....	499
Commands	499
Error messages	509
Return codes	515
Using task profiles	526

Contacting Technical Support.....	529
How to obtain technical support.....	530
Technical support by phone.....	530
Technical Support via Kaspersky CompanyAccount	531
Collecting information for Technical Support	532
Creating a trace file	533
Contents and storage of trace files.....	534
Enabling or disabling transmission of dump files and trace files to Kaspersky Lab	537
Sending files to the Technical Support server	537
Enabling and disabling protection of dump files and trace files	538

About Kaspersky Endpoint Security for Windows

This section describes the functions, components, and distribution kit of Kaspersky Endpoint Security 10 for Windows, further referred to as Kaspersky Endpoint Security, and provides a list of hardware and software requirements of Kaspersky Endpoint Security.

In this section:

Distribution kit	5
Hardware and software requirements.....	6
User and administrator roles in the application.....	7

Distribution kit

The Kaspersky Endpoint Security distribution kit contains the following files:

- Files that are required for installing the application using any of the available methods:
- Update package files used during installation of the application.
- The klcfginst.msi file for installing the Kaspersky Endpoint Security administration plug-in via Kaspersky Security Center.
- The ksn_<language ID>.txt file, which you can view to look through the terms of participation in Kaspersky Security Network.
- The license.txt file, with which you can view the End User License Agreement.
- The incompatible.txt file that contains a list of incompatible software.

- The installer.ini file that contains the internal settings of the distribution kit.

It is not recommended to change the values of these settings. If you want to change installation options, use the setup.ini file.

You must unpack the distribution kit to access the files.

Hardware and software requirements

To ensure proper operation of Kaspersky Endpoint Security, your computer must meet the following requirements:

Minimum general requirements:

- 2 GB of free disk space on the hard drive
- Microsoft® Internet Explorer® 7.0
- An Internet connection for activating the application and updating databases and application modules
- 2 GB of free RAM
- Intel Pentium processor (or compatible equivalent):
 - For a 32-bit operating system - Intel Pentium 1 GHz
 - For a 64-bit operating system - Intel Pentium 2 GHz

Supported operating systems for workstations:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
- Microsoft Windows 8 Professional / Enterprise x86 Edition, Microsoft Windows 8 Professional / Enterprise x64 Edition, Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition

- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition

For details about support for the Microsoft Windows 10 operating system, please refer to article 13036 in the Technical Support Knowledge Base:

<http://support.kaspersky.com/kes10wks> <http://support.kaspersky.com/kes10wks>.

Supported operating systems for file servers:

- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1, Microsoft Windows Server 2008 Standard / Enterprise x86 Edition SP2, Microsoft Windows Server 2008 Standard / Enterprise x64 Edition SP2
- Microsoft Windows Small Business Server 2011 Essentials / Standard x64 Edition
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition, Microsoft Windows MultiPoint Server 2012 x64 Edition
- Microsoft Windows Server 2016

For details about support for the Microsoft Windows Server 2016 operating system, please refer to article 13036 in the Technical Support Knowledge Base:

<http://support.kaspersky.com/kes10fs> <http://support.kaspersky.com/kes10fs>.

Environment and operation requirements

To ensure user data security and maximize protection efficiency that is provided by Kaspersky Endpoint Security several other requirements had to be observed.

Attacker access protection

The device secured by the TOE should not fall under temporary and undetected physical control of an attacker when the device is booted. Potential attacker must not have physical or logical access to the device secured by the TOE before and during the TOE installation. Appropriate physical security measures and physical security policies have to be in place.

Correct behaviour of authorised users

Authorised users shall not actively compromise the security of the device secured by the TOE and the TOE itself and should be instructed not to leave a device secured by the TOE while it is switched on and running.

TOE secure operation

Non-trusted software (especially with ability to perform direct access to the hard disk) is not installed and will not be installed on the device secured by the TOE. The users are instructed not to install or use utility programs like partition managers or disk copy programs.

Password protection

All authorised individuals (users, administrators) protect their passwords and/or PINs for Token to avoid disclosure. They are instructed to keep their password secret and not to write down their password, neither manually nor electronically. Unauthorised individuals shall not get the password of an authorised individual. The corresponding security measures sufficiently protect against password/PIN eaves dropping and recording using software tools or additional hardware devices. In particular, the devices and the environment shall be protected against installing any software programs or hardware devices, which enable capturing user password inputs on the keyboard.

Trusted administration

The administrators responsible for the device and KSC server administration have to be trustworthy. They perform all tasks correctly regarding the TOE security.

User and administrator roles in the application

Kaspersky Endpoint Security supports two user roles: User and Administrator.

User is associated with Administrator role when he enters valid username and password when performing operations in GUI or Command Line interface. Additionally all actions done through Kaspersky Security Center are also attributed to Administrator role.

Username and password are defined via Kaspersky Security Center Policy. See section Password Protection Windows on page 477.

The Administrator role performs installation, configuration and administration of Kaspersky Endpoint Security locally through GUI and command line interface or remotely using the Kaspersky Security Center Administration Server and the Kaspersky Endpoint Security administration plug-in.

A user can perform the following actions in the local interface of Kaspersky Endpoint Security:

- Run a custom scan task.
- Send the administrator requests for access provision in case devices, applications or web resources necessary for work are being blocked, or to obtain access to encrypted files.
- Configure application settings if their modification is allowed by the Kaspersky Security Center policy or if the user's computer is not running under a policy.

In a client computer with Kaspersky Endpoint Security installed is running under a Kaspersky Security Center policy, the administrator can restrict availability of operations or settings with the application to the User. In this case, the application will prompt the user for the password when the user attempts to perform a protected operation in the Kaspersky Endpoint Security local interface. See section Password Protection Windows on page 477.

License and activation

Administrators should maintain active license for Kaspersky Endpoint for Windows at all times to ensure lasting data protection.

Please refer to section Key addition task settings section on p. 491 below for instruction how to add activation keys when active license expire. Kaspersky Endpoint Security for Windows have option to include backup activation keys to ensure uninterrupted protection due to license expiration.

If the license has expired, the application does not encrypt new data, and old encrypted data remains encrypted and available for use. In this event, encrypting new data requires the program be activated with a new license that permits the use of encryption. The rest of functionality stays the same.

Managing the application on a client computer

This section contains information on how to work with the application by using the local interface on the client computer of the user.

In this section:

Application functions in the Windows context menu	11
Web Control	13
Application Privilege Control	46
Application Startup Control.....	84
Device Control	112
Anti-Virus protection.....	134
Working with encrypted devices when there is no access to them	242

Application functions in the Windows context menu

Kaspersky Endpoint Security is integrated into the Windows context menu. Using the context menu of any file on the computer, the user can perform the following operations with a file:

- **Scan for viruses.**

Selecting this item starts a custom scan task. Kaspersky Endpoint Security runs a virus scan on the file from whose context menu the task was started.

- **Check reputation in KSN.**

When this item is selected, Kaspersky Endpoint Security sends a file reputation request to the KSN server. In the **<File name> - Reputation in KSN** window that opens, the user can view the following information about the selected file:

- **Path.** Path in which the file is saved to disk.
 - **Version.** Application version (information is displayed only for executable files).
 - **Digital signature.** Presence of a digital signature with the file.
 - **Signed.** Date on which the file was signed with a digital signature.
 - **Created.** File creation date.
 - **Modified.** Date of last modification of the file.
 - **Size.** Disk space occupied by the file.
 - Information about how many users trust the file and how many users block the file.
- **Add to encrypted package.**

When this item is selected, Kaspersky Endpoint Security places the file into a self-extracting password-protected encrypted package.

Application icon context menu

The context menu of the application icon contains the following items:

- **Kaspersky Endpoint Security 10 for Windows.** Opens the **Protection and Control** tab in the main application window. The **Protection and Control** tab lets you adjust the operation of application components and tasks, and view the statistics of processed files and detected threats.
- **Settings.** Opens the **Settings** tab in the application window. The Settings tab lets you change the default application settings.
- **Pause protection and control / Resume protection and control.** Temporarily pauses / resumes the operation of protection and control components. This context menu item does not affect the update task and scan tasks, being only available when the Kaspersky Security Center policy is disabled.
- **Disable policy / Enable policy.** Disables / enables the Kaspersky Security Center policy. This context menu item is available when Kaspersky Endpoint Security operates under a policy, and a password for disabling the Kaspersky Security Center policy has been set.
- **About.** This item opens an information window with application details.
- **Exit.** This item quits Kaspersky Endpoint Security. Clicking this context menu item causes the application to be unloaded from the computer RAM.



Application icon context menu

You can open the context menu of the application by resting the pointer on the application icon in the taskbar notification area of Microsoft Windows and right-clicking.

Web Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Web Control and instructions on how to configure the component settings.

In this section:

About Web Control.....	14
Web Control subsection	30

About Web Control

Web Control allows controlling actions by LAN users, by restricting or blocking access to web resources.

A web resource is an individual web page or several web pages, or a website or several websites that have a common feature.

Web Control provides the following options:

- Saving traffic.

Traffic is controlled by restricting or blocking downloads of multimedia files, or by restricting or blocking access to web resources that are unrelated to users' job responsibilities.

- Delimiting access by content categories of web resources.

To save traffic and reduce potential losses from the misuse of employee time, you can restrict or block access to specific categories of web resources (for example, block access to web resources that belong to the "Internet communication media" category).

- Centralized control of access to web resources.

When using Kaspersky Security Center, personal and group settings of access to web resources are available.

All restrictions and blocks that are applied to access to web resources are implemented as rules of access to web resources.

Web resource content categories

The web resource content categories (hereinafter also referred to as "categories") listed below have been selected to most fully describe the blocks of data hosted by web resources, taking into account their functional and thematic features. The order in which the categories appear in this list does not reflect the relative importance or prevalence of such categories on the Internet. The category names are provisional and used solely for purposes of Kaspersky Lab products and websites. The names do not necessarily reflect the meaning implied by law. One web resource can belong to several categories at once.

Adult content

This category includes the following types of web resources:

- Web resources containing any photo or video materials depicting genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources containing any text materials, including literary or artistic materials, describing genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources devoted to a discussion of the sexual aspect of human relations.

Overlaps the "Internet communication media" category.

- Web resources containing erotic materials, works that provide a realistic portrayal of sexual behavior of humans, or works of art designed to stimulate sexual arousal.

- Web resources of official media outlets and online communities with an established target audience, containing a special section and/or individual articles devoted to the sexual aspect of human relations.
- Web resources devoted to sexual perversions.
- Web resources that advertise and sell items for use in sex and stimulation of sexual arousal, sexual services and intimate dating, including services provided online via erotic video chats, "telephone sex", "sexting" ("virtual sex").

Overlaps the "Electronic commerce" category.

This category does not include web resources with scientific, medical, and scholarly content.

Software, audio, video

This category includes the following subcategories that you can individually select:

- **Audio and video.**

This subcategory includes web resources distributing audio and video materials: movies, recordings of sports broadcasts, recordings of concerts, songs, movie clips, videos, tutorial audio and video recordings, etc.

- **Torrents.**

This subcategory includes websites of torrent trackers intended for sharing files of unlimited size.

- **File sharing.**

This subcategory includes file sharing websites irrespective of the physical location of files being distributed.

Alcohol, tobacco, narcotics

This category includes web resources whose content is directly or indirectly related to alcoholic or alcohol-containing products, tobacco products, and narcotic, psychotropic and/or intoxicating substances.

- Web resources that advertise and sell such substances and paraphernalia for consuming them.

Overlaps the "Electronic commerce" category.

- Web resources with instructions on how to consume or produce narcotic, psychotropic, and/or intoxicating substances.

This category includes web resources addressing scientific and medical topics.

Violence

This category includes web resources containing any photo, video or text materials describing acts of physical or psychological violence directed against human beings, or cruel treatment of animals.

- Web resources depicting or describing scenes of executions, torture, or abuse, as well as tools intended for such practices.

Overlaps the "Weapons, explosives, pyrotechnics" category.

- Web resources depicting or describing scenes of murder, fighting, battery, or rape, scenes in which humans, animals, or imaginary creatures are abused or humiliated.
- Web resources with information inciting acts that jeopardize life and/or health, including self-harm or suicide.
- Web resource with information substantiating or justifying the admissibility of violence and/or cruelty, or inciting violent acts against humans or animals.
- Web resources with particularly realistic portrayals or descriptions of victims and atrocities of war, armed conflicts, and military clashes, accidents, catastrophes, natural disasters, industrial or social cataclysms, or human suffering.
- Browser computer games with scenes of violence and cruelty, including the so-called "shooters", "fightings", "slashers", etc.

Overlaps the "Computer games" category.

Weapons, explosives, pyrotechnics

This category includes web resources with information about weapons, explosives, and pyrotechnical products:

- Websites of weapons, explosives, and pyrotechnical products manufacturers and stores.

Overlaps the "Electronic commerce" category.

- Web resources devoted to the manufacture or use of weapons, explosives, and pyrotechnical products.
- Web resources containing analytical, historical, manufacturing, and encyclopedic materials devoted to weapons, explosives, and pyrotechnical products.

The term "weapons" means appliances, items, and means designed to harm the life or health of humans and animals and/or damage equipment and structures.

Profanity

This category includes web resources where profane language has been detected.

Overlaps the "Adult content" category.

This category also includes web resources with linguistic and philological materials containing profanity as the subject of study.

Gambling, lotteries, sweepstakes

This category includes web resources that offer users to participate financially in gambling, even if such financial participation is not a mandatory condition for access to the website. This category includes web resources offering:

- Gambling in which participants are required to make monetary contributions.

Overlaps the "Computer games" category.

- Sweepstakes that involve betting with money.
- Lotteries that involve purchasing lottery tickets or numbers.
- Information that can trigger the desire to participate in gambling, sweepstakes, and lotteries.

Overlaps the "Electronic commerce" category.

This category includes games that offer free-of-charge participation as a separate mode, as well as web resources that actively advertise web resources falling into this category to users.

Network Communications

This category includes web resources that enable users (whether registered or not) to send personal messages to other users of the relevant web resources or other online services and/or add content (either open to public access or restricted) to the relevant web resources on certain terms. You can individually select the following subcategories:

- **Chats and forums.**

This subcategory includes web resources intended for public discussion of various topics using special web applications, as well as web resources designed to distribute or support instant messaging applications that enable real-time communication.

- **Blogs.**

This subcategory includes blog platforms, which are websites that provide paid or free services for creating and maintaining blogs.

- **Social networks.**

This subcategory includes websites designed for building, displaying, and managing contacts between persons, organizations, and governments, which require registration of a user account as a condition of participation.

- **Dating sites.**

This subcategory includes web resources serving as a variety of social networks providing paid or free services.

Overlaps the "Adult content" and "Electronic commerce" categories.

- **Web-based mail.**

This subcategory includes exclusively login pages of an email service and mailbox pages containing emails and associated data (such as personal contacts). This category does not include other web pages of an Internet service provider that also offers email service.

E-tailers, banks, and payment systems

This category includes web resources designed for any online transactions in non-cash monetary funds using special-purpose web applications. You can individually select the following subcategories:

- **Shops and auctions.**

This subcategory includes online shops and auctions selling any goods, work or services to individuals and/or legal entities, including websites of stores that conduct sales exclusively online and online profiles of physical stores that accept online payments.

- **Banks.**

This subcategory includes specialized web pages of banks with online banking functionality, including wire (electronic) transfers between bank accounts, making bank deposits, performing currency conversion, paying for third-party services, etc.

- **Payment systems.**

This subcategory includes web pages of e-money systems that provide access to the user's personal account.

In technical terms, payment can be effected using both bank cards of any types (plastic or virtual, debit or credit, local or international) and e-money. Web resources can fall into this category regardless of whether or not they have such technical aspects as data transmission over the SSL protocol, the use of 3D Secure authentication, etc.

Job search

This category includes web resources designed to bring together employers and job seekers:

- Websites of recruitment agencies (employment agencies and/or headhunting agencies).
- Websites of employers with descriptions of available job openings and their advantages.
- Independent portals with offers of employment from employers and recruitment agencies.
- Professional social networks that, among all else, make it possible to publish or find information about specialists who are not actively searching for employment.

Overlaps the "Internet communication media" category.

Anonymous access systems

This category includes web resources that act as an intermediary in downloading content of other web resources using special web applications for purposes of:

- Bypassing restrictions imposed by a LAN administrator on access to web addresses or IP addresses;
- Anonymously accessing web resources, including web resources that specifically reject HTTP requests from certain IP addresses or their groups (for example, IP addresses grouped by country of origin).

This category includes both web resources intended exclusively for the above mentioned purposes ("anonymizers") and web resources with technically similar functionality.

Computer games

This category includes web resources devoted to computer games of various genres:

- Websites of computer game developers.
- Web resources devoted to a discussion of computer games.

Overlaps the "Internet communication media" category.

- Web resources providing the technical capability for online participation in gaming, together with other participants or individually, with local installation of applications or without such installation ("browser games").
- Web resources designed to advertise, distribute, and support gaming software.

Overlaps the "Electronic commerce" category.

Religions, religious associations

This category includes web resources with materials on public movements, associations, and organizations with a religious ideology and/or cult in any manifestations.

- Websites of official religious organizations at different levels, from international religions to local religious communities.

- Websites of unregistered religious associations and societies that historically emerged by splintering from a dominant religious association or community.
- Websites of religious associations and communities that have emerged independently of traditional religious movements, including at the initiative of a specific founder.
- Websites of inter-confessional organizations pursuing cooperation among representatives of different traditional religions.
- Web resources with scholarly, historical, and encyclopedic materials on the subject of religions.
- Web resources with detailed portrayals or descriptions of the worship as part of religious cults, including rites and rituals involving the worship of God, beings and/or items believed to have supernatural powers.

News media

This category includes web resources with public news content created by the mass media or online publications that let users add their own news reports:

- Websites of official media outlets.
- Websites offering information services with the attribution of official sources of information.
- Websites offering aggregation services, of collections of news information from various official and unofficial sources.
- Websites where news content is created by users themselves ("social news sites").

Overlaps the "Internet communication media" category.

Banners

This category includes web resources with banners. Advertising information on banners may distract users from their activities, while banner downloads increase the amount of traffic.

The web resource content categories (hereinafter also referred to as "categories") listed below have been selected to most fully describe the blocks of data hosted by web resources, taking into account their functional and thematic features. The order in which the categories appear in this list does not reflect the relative importance or prevalence of such categories on the Internet. The category names are provisional and used solely for purposes of Kaspersky Lab products and

websites. The names do not necessarily reflect the meaning implied by law. One web resource can belong to several categories at once.

Adult content

This category includes the following types of web resources:

- Web resources containing any photo or video materials depicting genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources containing any text materials, including literary or artistic materials, describing genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources devoted to a discussion of the sexual aspect of human relations.

Overlaps the "Internet communication media" category.

- Web resources containing erotic materials, works that provide a realistic portrayal of sexual behavior of humans, or works of art designed to stimulate sexual arousal.
- Web resources of official media outlets and online communities with an established target audience, containing a special section and/or individual articles devoted to the sexual aspect of human relations.
- Web resources devoted to sexual perversions.
- Web resources that advertise and sell items for use in sex and stimulation of sexual arousal, sexual services and intimate dating, including services provided online via erotic video chats, "telephone sex", "sexting" ("virtual sex").

Overlaps the "Electronic commerce" category.

This category does not include web resources with scientific, medical, and scholarly content.

Software, audio, video

This category includes the following subcategories that you can individually select:

- **Audio and video.**

This subcategory includes web resources distributing audio and video materials: movies, recordings of sports broadcasts, recordings of concerts, songs, movie clips, videos, tutorial audio and video recordings, etc.

- **Torrents.**

This subcategory includes websites of torrent trackers intended for sharing files of unlimited size.

- **File sharing.**

This subcategory includes file sharing websites irrespective of the physical location of files being distributed.

Alcohol, tobacco, narcotics

This category includes web resources whose content is directly or indirectly related to alcoholic or alcohol-containing products, tobacco products, and narcotic, psychotropic and/or intoxicating substances.

- Web resources that advertise and sell such substances and paraphernalia for consuming them.

Overlaps the "Electronic commerce" category.

- Web resources with instructions on how to consume or produce narcotic, psychotropic, and/or intoxicating substances.

This category includes web resources addressing scientific and medical topics.

Violence

This category includes web resources containing any photo, video or text materials describing acts of physical or psychological violence directed against human beings, or cruel treatment of animals.

- Web resources depicting or describing scenes of executions, torture, or abuse, as well as tools intended for such practices.

Overlaps the "Weapons, explosives, pyrotechnics" category.

- Web resources depicting or describing scenes of murder, fighting, battery, or rape, scenes in which humans, animals, or imaginary creatures are abused or humiliated.

- Web resources with information inciting acts that jeopardize life and/or health, including self-harm or suicide.
- Web resource with information substantiating or justifying the admissibility of violence and/or cruelty, or inciting violent acts against humans or animals.
- Web resources with particularly realistic portrayals or descriptions of victims and atrocities of war, armed conflicts, and military clashes, accidents, catastrophes, natural disasters, industrial or social cataclysms, or human suffering.
- Browser computer games with scenes of violence and cruelty, including the so-called "shooters", "fightings", "slashers", etc.

Overlaps the "Computer games" category.

Weapons, explosives, pyrotechnics

This category includes web resources with information about weapons, explosives, and pyrotechnical products:

- Websites of weapons, explosives, and pyrotechnical products manufacturers and stores.

Overlaps the "Electronic commerce" category.

- Web resources devoted to the manufacture or use of weapons, explosives, and pyrotechnical products.
- Web resources containing analytical, historical, manufacturing, and encyclopedic materials devoted to weapons, explosives, and pyrotechnical products.

The term "weapons" means appliances, items, and means designed to harm the life or health of humans and animals and/or damage equipment and structures.

Profanity

This category includes web resources where profane language has been detected.

Overlaps the "Adult content" category.

This category also includes web resources with linguistic and philological materials containing profanity as the subject of study.

Gambling, lotteries, sweepstakes

This category includes web resources that offer users to participate financially in gambling, even if such financial participation is not a mandatory condition for access to the website. This category includes web resources offering:

- Gambling in which participants are required to make monetary contributions.

Overlaps the "Computer games" category.

- Sweepstakes that involve betting with money.
- Lotteries that involve purchasing lottery tickets or numbers.
- Information that can trigger the desire to participate in gambling, sweepstakes, and lotteries.

Overlaps the "Electronic commerce" category.

This category includes games that offer free-of-charge participation as a separate mode, as well as web resources that actively advertise web resources falling into this category to users.

Network Communications

This category includes web resources that enable users (whether registered or not) to send personal messages to other users of the relevant web resources or other online services and/or add content (either open to public access or restricted) to the relevant web resources on certain terms. You can individually select the following subcategories:

- **Chats and forums.**

This subcategory includes web resources intended for public discussion of various topics using special web applications, as well as web resources designed to distribute or support instant messaging applications that enable real-time communication.

- **Blogs.**

This subcategory includes blog platforms, which are websites that provide paid or free services for creating and maintaining blogs.

- **Social networks.**

This subcategory includes websites designed for building, displaying, and managing contacts between persons, organizations, and governments, which require registration of a user account as a condition of participation.

- **Dating sites.**

This subcategory includes web resources serving as a variety of social networks providing paid or free services.

Overlaps the "Adult content" and "Electronic commerce" categories.

- **Web-based mail.**

This subcategory includes exclusively login pages of an email service and mailbox pages containing emails and associated data (such as personal contacts). This category does not include other web pages of an Internet service provider that also offers email service.

E-tailers, banks, and payment systems

This category includes web resources designed for any online transactions in non-cash monetary funds using special-purpose web applications. You can individually select the following subcategories:

- **Shops and auctions.**

This subcategory includes online shops and auctions selling any goods, work or services to individuals and/or legal entities, including websites of stores that conduct sales exclusively online and online profiles of physical stores that accept online payments.

- **Banks.**

This subcategory includes specialized web pages of banks with online banking functionality, including wire (electronic) transfers between bank accounts, making bank deposits, performing currency conversion, paying for third-party services, etc.

- **Payment systems.**

This subcategory includes web pages of e-money systems that provide access to the user's personal account.

In technical terms, payment can be effected using both bank cards of any types (plastic or virtual, debit or credit, local or international) and e-money. Web resources can fall into this category regardless of whether or not they have such technical aspects as data transmission over the SSL protocol, the use of 3D Secure authentication, etc.

Job search

This category includes web resources designed to bring together employers and job seekers:

- Websites of recruitment agencies (employment agencies and/or headhunting agencies).
- Websites of employers with descriptions of available job openings and their advantages.
- Independent portals with offers of employment from employers and recruitment agencies.
- Professional social networks that, among all else, make it possible to publish or find information about specialists who are not actively searching for employment.

Overlaps the "Internet communication media" category.

Anonymous access systems

This category includes web resources that act as an intermediary in downloading content of other web resources using special web applications for purposes of:

- Bypassing restrictions imposed by a LAN administrator on access to web addresses or IP addresses;
- Anonymously accessing web resources, including web resources that specifically reject HTTP requests from certain IP addresses or their groups (for example, IP addresses grouped by country of origin).

This category includes both web resources intended exclusively for the above mentioned purposes ("anonymizers") and web resources with technically similar functionality.

Computer games

This category includes web resources devoted to computer games of various genres:

- Websites of computer game developers.
- Web resources devoted to a discussion of computer games.

Overlaps the "Internet communication media" category.

- Web resources providing the technical capability for online participation in gaming, together with other participants or individually, with local installation of applications or without such installation ("browser games").
- Web resources designed to advertise, distribute, and support gaming software.

Overlaps the "Electronic commerce" category.

Religions, religious associations

This category includes web resources with materials on public movements, associations, and organizations with a religious ideology and/or cult in any manifestations.

- Websites of official religious organizations at different levels, from international religions to local religious communities.
- Websites of unregistered religious associations and societies that historically emerged by splintering from a dominant religious association or community.
- Websites of religious associations and communities that have emerged independently of traditional religious movements, including at the initiative of a specific founder.
- Websites of inter-confessional organizations pursuing cooperation among representatives of different traditional religions.
- Web resources with scholarly, historical, and encyclopedic materials on the subject of religions.
- Web resources with detailed portrayals or descriptions of the worship as part of religious cults, including rites and rituals involving the worship of God, beings and/or items believed to have supernatural powers.

News media

This category includes web resources with public news content created by the mass media or online publications that let users add their own news reports:

- Websites of official media outlets.

- Websites offering information services with the attribution of official sources of information.
- Websites offering aggregation services, of collections of news information from various official and unofficial sources.
- Websites where news content is created by users themselves ("social news sites").

Overlaps the "Internet communication media" category.

Banners

This category includes web resources with banners. Advertising information on banners may distract users from their activities, while banner downloads increase the amount of traffic.

Web Control subsection

In this window, the administrator can perform the following tasks:

- Enable or disable Web Control.
- Use rules to restrict user access to web resources.
- Run diagnostics on created rules of access to web resources.
- Form templates for messages about events that occurred during the operation of Web Control.

The following settings are available:

Enable Web Control

This check box enables / disables the Web Control component.

If the check box is selected, Kaspersky Endpoint Security controls access to websites and their content by all users.

The check box is selected by default.

Add

This button opens the **Rule of access to web resources** window. You can create a new rule in this window.

Edit

This button opens the **Rule of access to web resources** window. You can edit the settings of the selected rule in this window.

This button is available if the rule selected in the list of rules is other than the default rule.

Delete

This button deletes the selected rule.

This button is available if the rule selected in the list of rules is other than the default rule.

Move up

This button moves the selected rule one rank up on the list of rules.

The higher a rule is on the list of rules, the higher priority it has.

Move down

This button moves the selected rule one rank down in the list of rules.

The lower a rule is on the list of rules, the lower priority it has.

Search field

A field for entering a query to search for web resource access rules in the table of access rules sorted by priority. In this field, you can enter the entire contents or any number of characters from the contents of the **Status**, **Rule name**, and **Users** columns.




To view the search results in sequence, use the ◀ and ▶ buttons.

Access rules sorted by priority

A table with web resource access rules.

The table contains the following columns:

- **Status**. This column displays the operating status of the rule:

- *On*. This status means that the rule is used when Web Control is enabled.
- *Off*. This status means that the rule is ignored when Web Control is enabled.
- **Rule name**. This column displays the name of the rule.
- **Users**. This column shows the names of users and / or user groups to which the rule applies.
- **Action**. This column shows the action that is performed by Kaspersky Endpoint Security. Kaspersky Endpoint Security performs this action if the user visits web resources that are described by the web resource access rule:
 - The  icon means that Kaspersky Endpoint Security allows access to web resources that are described by the rule.
 - The  icon means that Kaspersky Endpoint Security blocks access to web resources that are described by the rule.
 - The  icon means that Kaspersky Endpoint Security warns the user that visiting the web resources described by the rule is not recommended.

Diagnostics

This button opens the **Rules diagnostics** window. In this window, you can test web resource access rules.

Templates

This button opens the **Templates** window. In this window, you can edit the templates of the messages which are displayed when web resource access rules are triggered.

Rules diagnostics window

In this window, the administrator can run diagnostics on the created rules for user access to web resources.

The following settings are available:

Specify address

This check box includes / excludes testing of access rules for an individual web resource address in / from the rules diagnostics conditions.

If the check box is selected, the field for entering the address of a web resource is available. Note that the only rules that are tested by the diagnostics are rules whose filters include the entered web resource address.

If the check box is cleared, the field for entering the address of a web resource is not available.

This check box is selected by default.

Specify users and / or groups

This check box enables / disables inclusion of the name of a user and / or user group in the testing of web resource access rules.

If the check box is selected, the **Select** button is available. The **Select** button allows you to open the **Select Users or Groups** window in Microsoft Windows and then select a user and / or user group whose names are taken into account when testing the web resource access rules.

If the check box is cleared, the **Select** button is not available and the web resource access rules are tested for all users.

This check box is selected by default.

Filter content

This check box includes / excludes analysis of content categories and / or data type categories when testing web resource access rules.

If this check box is selected, the **By content categories / By types of data / By content categories and types of data** drop-down list is available.

This check box is selected by default.

By content categories / By types of data / By content categories and types of data

This drop-down list allows you to specify the type of web content filtering.

Possible list values:

- **By content categories.** If this option is selected, a list with the names of content categories is available.

You can select the check boxes next to the names of the content categories for which you want to filter web content.

By default, all check boxes on the list of content category names are cleared.

- **By types of data.** If this option is selected, a list with the names of data type categories is available.

You can select the check boxes next to the names of the data type categories for which you want to filter web content.

By default, all check boxes on the list of data type category names are cleared.

- **By content categories and types of data.** If this option is selected, lists with the names of content categories and data type categories are available.

You can select the check boxes next to the names of the content categories and data type categories for which you want to filter web content.

By default, all check boxes are cleared.

Include time of access attempt

This check box determines whether the time and day of the attempt to access the web resources specified in the rule diagnostics conditions are to be included in / excluded from the test of the web resource access rule.

This check box is selected by default.

Test

This button starts the testing of all currently existing web resource access rules.

After you click the **Test** button, a notification of the action that is performed by Kaspersky Endpoint Security (according to the first triggered rule) is displayed to the right of the button, while **The following rules will also be applied (in order of triggering)** table displays the actions that are performed by Kaspersky Endpoint Security according to the rules that are triggered after the first one.

The button is available if diagnostics conditions are specified.

The following rules will also be applied (in order of triggering)

This table displays information about the actions performed by Kaspersky Endpoint Security according to the second and subsequent rules that are triggered during diagnostics.

The table contains the following columns:

- **Rule name.** This column displays the name of the rule that was triggered during rules diagnostics.
- **Action.** This column displays information about the action that is performed by Kaspersky Endpoint Security according to the triggered rule.

Blockage tab

The entry field contains the template of the message that appears if a rule which blocks access to a web resource is triggered.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **User name (%USER_NAME%).** This variable is replaced with the name of the current account on the computer where the block message is displayed.
- **Web resource address (%CANONIC_REQUEST_URL%).** This variable is replaced with the normalized form of the address of the blocked web resource.
- **Rule name (%RULE%).** This variable is replaced with the name of the rule according to which the web resource is blocked.
- **Email for sending a message (%COMPLAIN_EMAIL%).** This variable is replaced with the email address specified in the **To** field of the complaint message template.

- **Name of content category (%CONTENT_CATEGORY_LIST%).** This variable is replaced with the name of the content category to which the blocked web resource belongs.
- **Name of data type category (%TYPE_CATEGORY_LIST%).** This variable is replaced with the name of the data type category to which the blocked web resource belongs.

Link

Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Message to administrator tab

The entry field contains the template of the message to be sent to the LAN administrator if the user considers the block to be a mistake.

You can edit the text of the template.

To

Field for entering the email address of the LAN administrator.

Subject

Field for entering the subject of the message.

The default subject is [WebControl] Mistaken blocking.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **User name (%USER_NAME%).** This variable is replaced with the name of the current account on the computer where the block message is displayed.

- **Web resource address (%CANONIC_REQUEST_URL%).** This variable is replaced with the normalized form of the address of the blocked web resource.
- **Rule name (%RULE%).** This variable is replaced with the name of the rule according to which the web resource is blocked.
- **Name of content category (%CONTENT_CATEGORY_LIST%).** This variable is replaced with the name of the content category to which the blocked web resource belongs.
- **Name of data type category (%TYPE_CATEGORY_LIST%).** This variable is replaced with the name of the data type category to which the blocked web resource belongs.

The method used to send messages and the choice of template depends on whether or not there is an active Kaspersky Security Center policy running on the computer with Kaspersky Endpoint Security installed. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Security Center installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Security Center installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage. The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.
 - If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.

- If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

Warning tab

The entry field consists of a template of the message that is displayed if a rule for warning about attempts to access an unwanted web resource is triggered.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **User name (%USER_NAME%).** This variable is replaced with the name of the current account on the computer where the block message is displayed.
- **Web resource address (%CANONIC_REQUEST_URL%).** This variable is replaced with the normalized form of the address of the blocked web resource.
- **Rule name (%RULE%).** This variable is replaced with the name of the rule according to which the web resource is blocked.
- **Email for sending a message (%COMPLAIN_EMAIL%).** The variable is replaced by the email address specified in the **To** field of the template.
- **Name of content category (%CONTENT_CATEGORY_LIST%).** This variable is replaced with the name of the content category to which the blocked web resource belongs.

- **Name of data type category (%TYPE_CATEGORY_LIST%).** This variable is replaced with the name of the data type category to which the blocked web resource belongs.
- **Link to requested web resource (%CONTINUE_PAGE%).** This variable is replaced with a link to the requested web page.
- **Link to web site (%CONTINUE_SITE%).** This variable is replaced with a link to the website on which the requested web page is located.
- **Link for access to domains (%CONTINUE_DOMAIN%).** This variable is replaced with a link to all existing domains on a level that is lower than or equal to the level marked with the * symbol.

For example, if the address of the blocked web page is `http://www.example.com`, the `%CONTINUE_DOMAIN%` variable is replaced with the link `http://*.example.com`. Clicking this link allows access to such web addresses as `http://www.example.com/*`, `http://domain.example.com/*`, `http://domain.domaine.example.com/*`, where the * wildcard replaces any sequence of zero or more characters.

Link

Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Rule of access to web resources window

In this window, the administrator can create a rule for user access to web resources.

A web resource access rule is a set of filters and actions that Kaspersky Endpoint Security performs when the user visits web resources that are described in the rule during the time span that is indicated in the rule schedule. Filters allow you to precisely specify a pool of web resources to which access is controlled by the Web Control component.

The following filters are available:

- **Filter by content.** Web Control categorizes web resources by content and data type. You can control user access to web resources with content and data types of certain categories. When the users visit web resources that belong to the selected content category and / or

data type category, Kaspersky Endpoint Security performs the action that is specified in the rule.

- **Filter by web resource addresses.** You can control user access to all web resource addresses or to individual web resource addresses and / or groups of web resource addresses.

If filtering by content and filtering by web resource addresses are specified, and the specified web resource addresses and / or groups of web resource addresses belong to the selected content categories or data type categories, Kaspersky Endpoint Security does not control access to all web resources in the selected content categories and / or data type categories. Instead, the application controls access only to the specified web resource addresses and / or groups of web resource addresses.

- **Filter by names of users and user groups.** You can specify the names of users and / or groups of users for which access to web resources is controlled according to the rule.

To create rules of access to web resources, the following settings are available:

Name

Field for entering the name of a web resource access rule.

If the name is not specified, the rule cannot be saved.

Filter content

This drop-down list allows you to set the type of filtering for web content which the user attempts to access.

Possible list values:

- **Any content.** If this value is selected, web content is not filtered.

This value is selected by default.

- **By content categories.** If this value is selected, web content is filtered by content categories and a list of content category names is available.

You can select the check boxes next to the names of the content categories for which you want to filter web content.

By default, all check boxes are cleared.

- **By types of data.** If this value is selected, web content is filtered by data type categories and a list of data type category names is available.

You can select the check boxes next to the names of the data type categories for which you want to filter web content.

By default, all check boxes are cleared.

- **By content categories and types of data.** If this value is selected, web content is filtered by content categories and data type categories; a list with the names of categories is also available.

You can select the check boxes next to the names of the content categories and data type categories for which you want to filter web content.

By default, all check boxes are cleared.

Apply to addresses

This drop-down list allows you to set the list of addresses of the web resources that are covered by the rule.

Possible list values:

- **To all addresses.** If this value is selected, the rule is applied to all addresses of web resources which the user attempts to access.

This value is set by default.

- **To individual addresses.** If this value is selected, the rule is applied to the following list of addresses of web resources.





You can edit, export, or import the list of addresses of web resources by using the following buttons:

- **Add.** This drop-down button allows you to add the address of a web resource or a group of addresses of web resources.
- **Edit.** This button allows you to edit the address of a web resource or a group of addresses of web resources.

This button is available if the address of a web resource or a group of addresses of web resources is selected from the list of addresses of web resources.

- **Delete.** This button allows you to delete the address of a web resource or a group of addresses of web resources.

This button is available if the address of a web resource or a group of addresses of web resources is selected from the list of addresses of web resources.

-  This button exports the entire list of addresses of web resources or its individual items into a .txt file.
-  This button imports the list of addresses of web resources from a .txt file.
-  When this button is clicked, the application copies the items that are selected from the list of addresses of web resources to the clipboard.
-  When this button is clicked, the application inserts elements from the clipboard into the list of addresses of web resources.

Specify users and / or groups

This check box enables / disables the inclusion of names of users and / or groups of users in the rule settings.

If the check box is selected, you can specify users and/or user groups whose access to web resources described by the rule is regulated by this rule. If the check box is selected but no user or user group is selected in the table, the rule cannot be saved.

If the check box is cleared, the rule applies to all users.

This check box is cleared by default.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. This window lets you select or modify users and/or user groups whose access to web resources described by the rule is regulated by this rule.

If the **Specify users and / or groups** check box is cleared, the **Select** button is not available, but the rule is valid for all users.

Action

This drop-down list allows you to set the action that Kaspersky Endpoint Security performs if the user attempts to access a web resource that matches the parameters of the rule.

Possible list values:

- **Allow** If this value is selected, Kaspersky Endpoint Security allows access to web resources that match the parameters of the rule.
- **Block** If this value is selected, Kaspersky Endpoint Security blocks access to web resources that match the parameters of the rule.
- **Warn.** If this value is selected, Kaspersky Endpoint Security displays a message to warn that a web resource is unwanted when the user attempts to access web resources that match the parameters of the rule. By using links from the warning message, the user can obtain access to the requested web resource.

Rule schedule

Drop-down list for selecting a rule schedule. By default, the list contains the **Always** item.

Settings

Clicking this button opens the **Rule schedule** window. In this window you can create a new rule schedule. The rule you have created will be added to the **Rule schedule** drop-down list.

Address / Address mask window

In this window, you can enter the address of a web resource or an address mask.

You can enter an address or web resource address mask in normalized or non-normalized form. If you enter an address or address mask in a non-normalized form, you are automatically prompted to normalize the entered web resource address or address mask.

Groups of addresses window

In this window, the administrator can specify a group of addresses to which the access rule should apply.

The following settings are available:

Groups of addresses of web resources

List of web resource address groups.

The check box opposite the name of the group of web resource addresses includes / excludes the group of web resource addresses in / from a web resource access rule.

Including or excluding a group of addresses in / from a web resource access rule expands or shortens the list of addresses of web resources that are covered by the rule. When the user opens a web resource, the rule manages access to this web resource if the address of the resource has been included in the group of addresses. This rule does not manage access to this web resource if the address of this web resource is not included in the group of addresses and does not fall within any of the selected content categories or data type categories.

Add

Button, which opens the **Group of addresses** window. In this window, you can create a new group of addresses of web resources.

Edit

Button, which opens the **Group of addresses** window. You can edit the settings of a group of addresses of web resources in this window.

The button is available if a group of addresses of web resources is selected.

Delete

This button deletes the selected group of addresses of web resources.

The button is available if a group of addresses of web resources is selected.

Rule schedule window

In this window, the administrator can specify a rule schedule. The rule schedule determines the time span during which Kaspersky Endpoint Security monitors access to web resources covered by the rule.

The following settings are available:

Name

A drop-down list that lets you select a rule schedule to edit the schedule or to use it as the basis for a new rule schedule.

Rename

Clicking this button opens the **Rule schedule name** window. This window lets you edit the name of a rule schedule.

Delete

This button deletes the rule schedule that is selected in the **Name** drop-down list.

Schedule of access to web resources

The rule schedule can be configured by using a special table. Table lines designate days of the week; table columns designate one-hour intervals in the time scale. Depending on the regional settings of the operating system, the time scale may be 24-hour or 12-hour.

The table cell colors reflect the time intervals that are included in, or excluded from, the schedule of the web resource access rule:

- Time intervals that are colored green are included in the rule schedule.
- Time intervals that are colored gray are excluded from the rule schedule.

Save as

Clicking this button opens the **Rule schedule name** window. This window lets you enter the name of the rule schedule to be created on the basis of the changes that are made to the rule schedule that is selected in the **Name** drop-down list.

Application Privilege Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Application Privilege Control and instructions on how to configure the component settings.

In this section:

About Application Privilege Control	46
Application Privilege Control subsection.....	47

About Application Privilege Control

Application Privilege Control prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources and to identity data.

This component controls the activity of applications, including their access to protected resources (such as files and folders, registry keys) by using *application control rules*. Application control rules are a set of restrictions that apply to various actions of applications in the operating system and to rights to access computer resources.

The network activity of applications is monitored by the Firewall component.

When an application is started for the first time, Application Privilege Control scans the application and places it in a trust group. A trust group defines the application control rules that Kaspersky Endpoint Security applies when controlling application activity.

We recommend that you participate in Kaspersky Security Network to make sure that Application Privilege Control is most effective. Data that is obtained through Kaspersky Security Network allows you to sort applications into groups with more accuracy and to apply optimum application control rules.

The next time the application starts, Application Privilege Control verifies the integrity of the application. If the application is unchanged, the component applies the current application control rules to it. If the application has been modified, Application Privilege Control re-scans it as if it were being started for the first time.

Application Privilege Control subsection

In this window, the administrator can perform the following tasks:

- Enable or disable Application Privilege Control.
- Configure rules for applications and protected resources.
- Configure the settings for assigning applications to trust groups.

The following settings are available:

Enable Application Privilege Control

This check box enables / disables operation of the Application Privilege Control component.

If the check box is selected, Application Privilege Control starts at Kaspersky Endpoint Security startup and registers the system activity of applications.

If the check box is cleared, Application Privilege Control is disabled.

This check box is selected by default.

Applications

This button opens the **Application control rules** tab in the **Application Privilege Control** window. This tab shows the list of applications access to which is monitored by Application Privilege Control. Applications are assigned to trust groups.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

Resources

This button opens the **Protected resources** tab in the **Application Privilege Control** window. This tab lets you view the list of personal data and operating system settings and resources to which Application Privilege Control controls access. You can also enable the protection of any resources in the list or add other resources to the list.

Update rules of previously unknown applications from KSN database

This check box enables / disables use of the Kaspersky Security Network database for updating the control rules for previously unknown applications.

If the check box is selected, Application Privilege Control updates the control rules for previously unknown applications by using the Kaspersky Security Network database.

This check box is selected by default.

Trust applications that have a digital signature

If this check box is selected, Application Privilege Control places digitally signed applications in the Trusted group.

If this check box is cleared, Application Privilege Control does not consider digitally signed applications to be trusted, and uses other parameters to determine their trust group.

This check box is selected by default.

Automatically move to group

If this option is selected, Application Privilege Control assigns an unknown application to the trust group that is selected in the **Low Restricted / High Restricted / Untrusted** drop-down list. The drop-down list is available if the **Automatically move to group** option is selected.

Use heuristic analysis to determine group

If this option is selected, Application Privilege Control uses heuristic analysis to determine the appropriate trust group for the unknown application.

This option is selected by default.

Maximum time to determine group

A field for entering the amount of time that is given to Application Privilege Control to heuristically analyze applications when they are started. The time period is specified in seconds.

By default, Application Privilege Control analyzes an application for 30 seconds. If Application Privilege Control cannot conclusively determine the danger rating of the application within this time, Application Privilege Control moves it to the "Low Restricted" trust group. Application Privilege Control continues to analyze the application in background mode and then assigns it to a specific trust group as determined through analysis.

Delete rules for applications that are not started for more than N days

This check box enables / disables the option to automatically delete application control rules for applications that have not been started for the specified time period. The time period is specified in days.

This check box is selected by default and Application Privilege Control deletes the control rules of applications that have not been started for more than 60 days.

Edit

Clicking this button opens the **Select trust group** window. This window lets you select a trust group according to whose rules the Firewall component will monitor the network activity of applications started before Kaspersky Endpoint Security.

Application control rules tab

In this window, the administrator can configure application control rules.

By default, application activity is controlled by application control rules that are defined for the trust group to which Kaspersky Endpoint Security assigned the application on first launch. If necessary, you can edit the application control rules for an entire trust group, for an individual application, or a group of applications that are within a trust group.

Application control rules that are defined for individual applications or groups of applications within a trust group have a higher priority than application control rules that are defined for a trust group. In other words, if the settings of the application control rules for an individual application or a group of applications within a trust group differ from the settings of application control rules for the trust group, the Application Privilege Control component controls the activity of the application or the group of applications within the trust group according to the application control rules that are for the application or the group of applications.

To create and modify application control rules, the following settings are available:

Application control rules

A table of control rules for applications that are categorized into trust groups. Kaspersky Endpoint Security follows the application control rules in regulating application access to operating system processes and resources.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,

- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is lower than 50,
- the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.






Such applications are subject to high restrictions on access to operating system resources.

You can sort the list of application control rules by trust group.

The context menu is available by right-clicking any column for the selected group of applications. From the context menu, you can do the following:

- Go to the application control rules or application group control rules.
- Create a subgroup within the application group.
- Restore the original settings of an application or group of applications (including all nested groups and applications).
- Delete an application or group of applications (not available for trust groups). When an application or group of applications is removed, the rules for this application or group of applications are removed from the table, and the Application Privilege Control and File Anti-Virus components no longer control the file and network activity of this application or of applications belonging to this group.
- Move an application to another trust group.

The table contains the following columns:

- **Application.** This column displays the names of the trust groups together with the applications and application groups assigned to them.
- **Vendor.** This column shows the name of the application vendor.
- **Group.** This column shows the icon of the trust group to which Application Privilege Control or the user has assigned the application:
 - Icon . Trusted.
 - Icon . Low Restricted.
 - Icon . High Restricted.
 - Icon . Untrusted.
 - Icon . The settings of the application control rule have been modified by the user.
- **Popularity.** This column shows the number of Kaspersky Security Network members that use this application.

Edit

This button opens the **Application control rules** or **Application group control rules** window. You can edit application control rules or application group control rules in this window.

This button is available when an application or group of applications is selected in the **Application control rules** table.

In the section located in the lower part of the window, you can view application details and change its trust group. This section is available when an application is selected in the list.

Group: Trusted / Low Restricted / High Restricted / Untrusted

The link designates the trust group to which the application is assigned.

Click the link to open the context menu. In the context menu, you can select a different trust group for this application. After you change the trust group, the application is automatically moved to the selected trust group in the list of application control rules.

Additional

Clicking the button opens the **Application control rules** window. This window lets you configure the rights of application access to monitored operating system resources and configure the network rules of this application.

File tab

In this window, you can view the following information about the executable file of an application:

Path

Path to the executable file of an application.

Vendor

Application vendor.

Application

Application name.

Product version

Version number of the installed application.

Size

Size of the executable file of the application.

Created

Application executable file creation date and time.

Modified

Application executable file modification date and time.

Status / Group

Trust group to which the application has been assigned by Kaspersky Endpoint Security or the user.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

Certificate status

Status of the certificate of a monitored application.

This information is available when the application is digitally signed.

The following setting values are possible:

- **Corrupted**
- **Revoked**
- **Untrusted.**
- **Expired**

- **Trusted (not verified)**
- **Trusted (verified)**
- **Absent**
- **Scan error**

Vendor

Certificate issuer.

Signature date

Digital signature creation date and time. This field is available when a digital signature exists.

Popularity

Number of users that use the application (based on the data that is received from Kaspersky Security Network).

Appeared in KSN

Date and time when the application first appeared on the computer of a Kaspersky Security Network participant.

Files and system registry tab

In this window, the administrator can configure the access of the selected application to files of the user and the operating system, and to the system registry.

The following settings are available:



Files and system registry

This table contains the rights of an application or application group to access operating system resources and identity data, which are combined into the **Files and system registry** category.

Operating system resources include system files, security settings, and various system services. They are combined into the **Operating system** category.

Personal data of the user includes user files and custom settings of applications. They are combined into the **Personal data** category.

Depending on whether or not the window has been opened from the context menu of the application or group of applications, the table lists the privileges of the application or application group to access operating system resources.

Access rights in the table are combined into groups that are presented hierarchically. You can display or hide entries of any group by clicking the  и  icons in the group header.




The table contains the following columns:

- **Resource.** This column shows the rights of an application or application group to access operating system resources and personal data of the user.

Entries in this column are sorted alphabetically by default. Groups and entries within each group are sorted alphabetically. A context menu in the column header lets you right-click to change the order of groups and entries within each group:

- **Sort ascending.** Selecting this command causes groups and values within each group to be sorted alphabetically.
- **Sort descending.** Selecting this command causes groups and values within each group to be sorted in reverse alphabetical order.
- **Read.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to read operating system resources and personal data of the user.
- **Write.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to modify and save existing resources of the operating system and personal data of the user.
- **Delete.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to delete operating system resources and personal data of the user.
- **Create.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to create and save new resources of the operating system and personal data of the user.

In the **Read**, **Write**, **Delete**, and **Create** columns, the selected right has a context menu that lets you right-click to modify the Kaspersky Endpoint Security action:

- The **Inherit** item signifies that the application or application group inherits the action of Kaspersky Endpoint Security from its parent group of rights. The displayed icon is identical to that of the parent group of rights.
- The  icon signifies that Kaspersky Endpoint Security allows the application or application group to access a process or resource of the operating system.
- The  icon signifies that Kaspersky Endpoint Security blocks the application or application group from accessing a process or resource of the operating system.
- The  icon signifies that, besides taking the specified action, Kaspersky Endpoint Security logs information about the attempt by an application or application group to access a process or resource of the operating system.



Rights tab

In this window, the administrator can configure the rights of the selected application to make modifications to the operation of the operating system.

The following settings are available:

Rights

This table lists the privileges of an application or group of applications to access processes and operating system resources depending on whether or not the window has been opened from the context menu of the application or group of applications.

Access rights in the table are combined into groups that are presented hierarchically. You can display or hide entries of any group. You can display entries of a group by clicking the  icon in the header of the group. You can hide entries of a group by clicking the  icon in the header of the group.



The table contains the following columns:

- **Resource.** This column displays the right of an application or application group to access processes and resources of the operating system.

Entries in this column are sorted alphabetically by default. Groups and entries within each group are sorted alphabetically. A context menu in the column header lets you right-click to change the order of groups and entries within each group:

- **Sort ascending.** Selecting this command causes groups and values within each group to be sorted alphabetically.
- **Sort descending.** Selecting this command causes groups and values within each group to be sorted in reverse alphabetical order.
- **Permission.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to access processes and resources of the operating system.

In this column, the selected right has a context menu that lets you right-click to modify the Kaspersky Endpoint Security action:

- The **Inherit** item signifies that the application or application group inherits the action of Kaspersky Endpoint Security from its parent group of rights. The displayed icon is identical to that of the parent group of rights.
- The  icon signifies that Kaspersky Endpoint Security allows the application or application group to access a process or resource of the operating system.
- The  icon signifies that Kaspersky Endpoint Security blocks the application or application group from accessing a process or resource of the operating system.
- The  icon signifies that, besides taking the specified action, Kaspersky Endpoint Security logs information about the attempt by an application or application group to access a process or resource of the operating system.

Network rules tab

In this window, the administrator can create network activity monitor rules for applications.

The following actions are available while managing application network rules:

- Create a new network rule.

The administrator can create a new network rule by which the Firewall must regulate the network activity of the application or applications that belong to the selected group of applications.

- Enable or disable a network rule.

All network rules are added to the list of network rules of applications with *Enabled* status. If a network rule is enabled, Firewall applies this rule.

The administrator can disable a network rule that was manually created. If a network rule is disabled, Firewall temporarily does not apply this rule.

- Change the settings of a network rule.

After the administrator creates a new network rule, he or she can always return to its settings and modify them as needed.

- Change the Firewall action for a network rule.

In the list of network rules, the administrator can edit the action that the Firewall applies for the network rule upon detecting network activity of this application or application group.

- Change the priority of a network rule.

The administrator can raise or lower the priority of a custom network rule.

- Delete a network rule.

The administrator can delete a custom network rule to stop the Firewall from applying this network rule to the selected application or application group upon detecting network activity, and to stop this rule from being displayed in the list of application network rules.

To work with network rules, the following settings are available:

Add

This button opens the **Network rule** window. You can create a new network rule in this window.

Edit

This button opens the **Network rule** window. You can edit the settings of the network rule in this window.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Delete

This button causes Firewall to delete the network rule that you select.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Firewall assigns an execution priority to each network rule. The priority of a network rule is determined by its position on the list of network rules. The topmost network rule in the list of network rules has the highest priority. Firewall processes network rules in the order in which they appear in the list of network rules, from top to bottom. Firewall locates the topmost rule that applies to the given network connection and executes it by either allowing or blocking network access.

Firewall ignores all subsequent network rules.

Move up

Clicking the button causes Firewall to move the selected network rule one line higher up on the list, thus increasing the rule's priority.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Move down

Clicking the button causes Firewall to move the selected network rule one line lower on the list, thus decreasing the rule's priority.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Network rules



This table contains information about network rules of an application or application group. In accordance with these rules, Firewall regulates the network activity of an application or application group.

The table shows information about application network rules, if the window is opened from the context menu of the application. Application network rules are used for imposing network activity

restrictions on a specific application. They factor in not only the characteristics of the network packet, but also the specific application to which this network packet is addressed or which issued this network packet. Such rules make it possible to fine-tune network activity filtering: for example, when a certain type of network connection is blocked for some applications but is allowed for others.

The table shows information about network rules of the application group, if the window is opened from the context menu of the application group. application group network rules have the same set of network activity restrictions that network rules for an application have. Firewall uses application group network rules for filtering the network activity of all applications within this group.

The table displays pre-configured network rules that are recommended by Kaspersky Lab for optimum protection of the network traffic of computers that run on Microsoft Windows operating systems. Such network rules are colored gray. The **Edit**, **Delete**, **Move up**, and **Move down** buttons are not available for them.

Some table columns include nested columns. You can open nested columns by clicking the  icon in the column header. You can hide nested columns by clicking the  icon in the column header.

The table contains the following columns:

Network service

The column contains a check box and name of the network service (value in the nested **Name** column). A *network service* is a collection of settings which describe the network activity for which you create a network rule.






The check box enables / disables the use of network rule.

When the check box is selected, Firewall applies this network rule.

When the check box is cleared, Firewall temporarily does not apply this network rule.

This column contains seven nested columns:


- **Name.** This column shows the name of a network service.
- **Direction.** This column shows an icon that indicates the direction of monitored network activity. The following network traffic directions are possible:



- Icon  – Inbound. Firewall applies a network rule to a network packet or data stream that is received by the user's computer.
- Icon  – Inbound (packet). Firewall applies the network rule to a network connection that is initiated by a remote computer.
- Icon  – Inbound / Outbound. Firewall applies the network rule to both inbound and outbound network packets or data streams, regardless of whether the user's computer or a remote computer initiated the network connection.
- Icon  – Outbound. Firewall applies a network rule to a network packet or data stream that leaves the user's computer.
- Icon  – Outbound (packet). Firewall applies the network rule to a network connection that is initiated by the user's computer.
- **Protocol.** This column shows the type of protocol for which Firewall monitors network connections.
- **Remote ports.** This column shows numbers of network ports of the remote computer.
- **Local ports.** This column shows numbers of network ports of the user's computer.
- **Network adapters.** This column shows the name of the adapter through which network traffic passes.
- **TTL.** This column shows the maximum time to live of outbound and/or inbound network packets that is specified in the network rule. A network rule controls the transmission of network packets whose time to live does not exceed the specified value.

Permission

This column shows the Firewall response on detecting network activity of an application or an application group that is subject to a network rule.

In this column, the selected network rule has a context menu. Right-click to bring it up and modify the Firewall action.

- The  icon signifies that Firewall allows access to the network resource.

- The  icon signifies that Firewall blocks access to the network resource.
- The  icon signifies that, besides taking the specified action, Firewall logs information about the attempt to access a network resource.

Address

This column shows the status of the network connection for which Firewall applies a network rule (the value of the nested **Remote addresses** column).

Firewall automatically detects the *network connection status* by analyzing network parameters. Depending on the network connection status, Firewall applies a set of network rules that are used for filtering network activity.

The network connection can have one of the following status types:

- **Public network.** This status is for networks that are not protected by any anti-virus applications, firewalls, or filters (for example, for Internet cafe networks). For the user of a computer that is connected to such a network, Firewall blocks access to files and printers of this computer. External users are also unable to access data through shared folders and remote access to the desktop of this computer. Firewall filters the network activity of each application according to the network rules that are set for it.

Firewall assigns *Public network* status to the Internet by default. You cannot change the status of the Internet.

- **Local network.** This status is assigned to networks whose users are trusted to access files and printers on this computer (for example, a LAN or home network).
- **Trusted network.** This status is intended for a safe network in which the computer is not exposed to attacks or unauthorized data access attempts. For networks with this status, Firewall permits any network activity within the given network.

This column contains two nested columns:

- **Local addresses.** This column does not contain any values because the **Local address** setting is not used when creating an application network rule or application group.
- **Remote addresses.** The column contains remote network addresses.

If the selected network rule is preset, the network rule settings are available for viewing only.

If the selected network rule is not preset, the network rule settings are displayed as links. Clicking any link opens the **Network rule** window, in which you can edit the network rule settings.

History tab


In this window, the administrator can view the history of application processing by Application Privilege Control.

The following information is available:

History

This table lists events or activities that occurred while access by applications or their child processes to operating system resources was monitored. Each line in the list of events contains information about the application or process and the action that was taken by Kaspersky Endpoint Security in response to an attempt by this application or process to access operating system resources.

You can filter the list of events by specifying the necessary filtering conditions:

- Clicking the  icon in the header of any column opens a context menu with a list of filtering conditions. You can specify the following filtering conditions for this column:
 - **(Custom)**. Selecting this item opens the **Custom filter** window. This window lets you specify a custom event filtering condition.
 - **(All)**. In selecting this item, you specify a filtering condition whereby event entries with any attribute values are displayed in the list.
 - **<Attribute value>**. By selecting one of the attribute values, you specify a filtering condition whereby the list of events displays only event entries that have the specified attribute value.

After you select a filtering condition, the list of events is refreshed and displays only those entries that match the filtering condition.



- Right-clicking the header of any column opens a context menu that lets you select the **Filter** command. Selecting this item opens the **Custom filter** window that lets you specify a custom event filtering condition.

- Right-clicking the header of any column opens a context menu that lets you specify the composition of columns to display in the list of events.
 - When the check box next to the column name is selected, this column is displayed in the list of events.
 - When the check box next to the column name is cleared, this column is hidden in the list of events.

You can sort the list of events by any column, by specifying the necessary sorting method. By default, the list of events is sorted in ascending order of values in the **Event date** column. For this column, an event with a later logging time is considered to have a greater value.

The header of each column has a context menu that lets you right-click to change the order of events:

- **Sort ascending.** Selecting this command causes values in any column, except the **Event date** column, to be sorted alphabetically. The values in the **Event date** column are sorted in ascending order.
- **Sort descending.** Selecting this command causes values in any column, except the **Event date** column, to be sorted in reverse alphabetical order. The values in the **Event date** column are sorted in descending order.

Some table columns include nested columns. You can open nested columns by clicking the  icon in the column header. You can hide nested columns by clicking the  icon in the column header.

The table consists of the following columns:

Event date

This column shows the event logging date and time.

Application

This column contains six nested columns:

- **Name.** This column shows the name of the executable file of the application.
- **Path.** This column shows the full path to the executable file of the application.

- **Process ID.** This column shows the unique process ID that the operating system assigns on application startup.
- **Parameters.** This column shows the initial parameters of the application.
- **Module.** This column shows the name of the dll module that made a call to the function to which a Kaspersky Endpoint Security task or component responded.
- **Function.** The name of a function of a third-party application to which a Kaspersky Endpoint Security task or component responded.

Component

This column shows the name of the component that processes the event.

Result

This column contains five nested columns:

- **Description.** This column describes the decision or action of the component at the time of the event.
- **Type.** This column indicates the type of data that is handled by the component at the time of the event.
- **Name.** This column shows the action requested by the object, the link, or path to the object that is handled by the component at the time of the event.
- **Threat level.** This column shows the threat level based on which the component makes a decision to handle the event.
- **Precision.** This column reflects the accuracy of the event-handling decision that is made by the component.

Action

This column reflects the action that is taken by the component at the time of handling the event.

Object

This column shows the name of the object on which the action is taken at the time of handling the event (combined values of the **Path** and **Name** columns). This column contains three nested columns:

- **Type.** This column indicates the type of object on which the action is taken at the time of the event.
- **Path.** This column indicates the location of the object on which the action is taken at the time of the event.
- **Name.** This column indicates the name of the object on which the action is taken at the time of the event.

Reason

This column indicates the reason for the result of event processing.

Exclusions tab

In this window, the administrator can exclude certain actions of the selected application from the application control rules.

The following settings are available:

Do not scan opened files

This check box enables / disables the exclusion of all files opened by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan the files that the application opens.

Do not monitor application activity

This check box enables / disables the monitoring of file and network activity of an application in the operating system by the Application Privilege Control, System Watcher, and Firewall components.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of the application.

Do not inherit restrictions of the parent process (application)

This check box enables / disables inheritance by the application of application control rules and application network rules that are specified for the parent process (application).

If the check box is selected, Kaspersky Endpoint Security monitors application activity according to the rules that are specified by the system administrator: file activity is monitored according to application control rules, while network activity is monitored according to application network rules.

If the check box is cleared, Kaspersky Endpoint Security monitors application activity according to application control rules and the application network rules that are inherited from the parent process (application).

Do not monitor child application activity

This check box enables / disables the monitoring of file and network activity of any child application of this application.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of child applications of this application.

Do not block interaction with the application interface

The check box enables / disables permission for the application to interact with the Kaspersky Endpoint Security interface.

If the check box is selected, the remote access application is allowed to manage Kaspersky Endpoint Security settings through the Kaspersky Endpoint Security interface.

Do not scan network traffic

This check box enables / disables the exclusion of network traffic generated by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan incoming and outgoing traffic of this application according to the network traffic exclusion settings. You can configure the exclusion settings in the section that is below the **Do not scan network traffic** setting.

In the section below the **Do not scan network traffic** setting, you can edit the settings of network traffic exclusion from virus scanning.

The section is available if the **Do not scan network traffic** check box is selected.

Any / specified remote IP addresses

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote IP addresses.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote IP addresses.

Clicking the **specify** link opens the **Remote IP addresses** window. This window lets you specify the list of IP addresses that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

Any / specified remote ports

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote ports.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote ports.

Clicking the **specify** link opens the **Remote ports** window. This window lets you specify the list of remote ports that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

Protected resources tab

In this window, the administrator can configure application rights to access various categories of operating system resources and personal data.

Kaspersky Lab specialists have established preset categories of protected resources. The administrator cannot edit or delete the preset categories of protected resources or the protected resources that are within these categories.

The administrator can perform the following actions:

- Add a new category of protected resources.
- Add a new protected resource.

- Disable protection of a resource.

The following settings are available:

Exclusions

Clicking the button opens the **Exclusions** window. This window lets you form a list of computer resources to which Application Privilege Control does not control access.

Search field

In the search field, you can type the entire contents or any number of characters from the contents of the **Protected resources** table columns. The search starts as you enter characters.

To reset the search results, delete the contents of the search field.

Everywhere / By application names / By resource names

The items in this drop-down list specify the scope of search in the table of applications and protected resources:

- **Everywhere.** If this item is selected, the search includes the contents of all columns in the **Protected resources** table.
- **By application names.** If this element is selected, the search is conducted in the contents of the **Application** column of the **Protected resources** table.
- **By resource names.** If this item is selected, the search includes the contents of the left part of the **Protected resources** table.

Add

Clicking this button opens a list.

The drop-down list includes the following items:

- **Category.** Selecting this item opens the **Category of protected resources** window. In this window you can enter the name of a category of protected resources to be added to the **Protected resources** table.

- **File or folder / Registry key.** Selecting this item opens the **Protected resource** window. This window lets you specify the settings of the resource that is being added to the **Protected resources** list.

Edit

This button opens the **Category of protected resources** or the **Protected resource** window. These windows let you edit the name of a category of protected resources or the settings of a resource that is added to the **Protected resources** table.

This button is available when a category of protected resources or a protected resource is selected in the **Protected resources** table.

You cannot modify the default category of protected resources or default protected resources.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete the category of protected resources or resource selected in the **Protected resources** table.

You cannot delete the default category of protected resources or default protected resources.

Update

Clicking this button sends a query to the Administration Server to update the list of protected resources.

This button is available only in the Administration Console of Kaspersky Security Center.

Protected resources

The list contains categorized computer resources. Application Privilege Control monitors attempts by other applications to access resources in the list.

A resource can be a category, file or folder, or registry key.

If the check box next to a resource is selected, Application Privilege Control protects the resource.

If the check box next to a resource is cleared, Application Privilege Control temporarily excludes it from the protection scope.

Rules of application access to protected resources

A table with rules defining the access of applications or groups of applications to protected resources.


The table contains the following columns:

- **Application.** This column displays the names of the trust groups together with the applications and application groups assigned to them. For these applications you can configure the rules of access to protected resources in the list on the left. The rule settings (read, write, delete, create) configured for a protected resource within a group apply to the entire group of protected resources.

You can sort the list of application control rules by values in this column. Besides trust groups, the elements that they contain (application groups and applications within each group) are also sorted. To sort the list of application control rules by values in this column, right-click to display the context menu of the appropriate column header and use the following commands:

- **Sort ascending.** Selecting this command causes the list of application control rules to be sorted by the **Application** column values in strict alphabetical order.
- **Sort descending.** Selecting this command causes the list of application control rules to be sorted by the **Application** column values in reverse alphabetical order.
- **Read.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or group of applications to read protected resources.
- **Write.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or group of applications to modify and save protected resources.
- **Delete.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or group of applications to delete protected resources.
- **Create.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to create and save new resources of the operating system and personal data of the user.

In the **Read**, **Write**, **Delete**, and **Create** columns, the selected right of access for an application or group of applications has a context menu that lets you right-click to modify the Kaspersky Endpoint Security action:

- The **Inherit** item signifies that the application or application group inherits the action of Kaspersky Endpoint Security from its parent group of rights. The displayed icon is identical to that of the parent group of rights.
- The  icon signifies that Kaspersky Endpoint Security allows the application or group of applications to access a group of protected resources.
- The  icon signifies that Kaspersky Endpoint Security blocks the application or group of applications from accessing a group of protected resources.
- The  icon signifies that, besides taking the specified action, Kaspersky Endpoint Security logs information about the attempt by an application or group of applications to access a group of protected resources.

The access right configured for a protected resource within a group applies to the entire group of protected resources.

Exclusions window

In this window, the administrator can form a list of exclusions. Access to resources added to the list of exclusions is not monitored by Application Privilege Control components. A file, folder, or registry key can be specified as a resource.

The following settings are available:

Exclusions

The table lists resources that have been excluded by the user from the protection scope of Application Privilege Control. A resource can be a file, folder, or registry key.

Resources that are added to the list of exclusions by default cannot be edited or deleted.

If the check box next to a resource is selected, Application Privilege Control does not control access to this resource.

If the check box next to a resource is cleared, Application Privilege Control protects the resource.

The table contains the following columns:

- **Resource.** This column shows the resource name.

- **Path.** This column shows the path to the resource.

The path may contain a mask.

Add

This button opens a context menu. You can select the type of resource in the context menu: file or folder or registry key. When a context menu item is selected, the **Protected resource** window opens. This window lets you specify the settings of the resource that is being added to the **Exclusions** list.

Edit

This button opens the **Protected resource** window. This window lets you modify the settings of the resource that is being added to the **Exclusions** list.

This button is available if an item is selected in the **Exclusions** list.

Delete

This button causes Kaspersky Endpoint Security to remove the selected item.

This button is available if an item is selected in the **Exclusions** list.

Protected resource window

In this window, the administrator can select a protected resource.

The following settings are available:

Name

Field for entering the name of a resource access to which should be protected by Application Privilege Control.

Path

Field that shows the path to a file or folder that is selected for addition to the list of protected resources.

This field is available when you add a file or folder as a protected resource.

Registry path

Field that shows the path in the registry tree to the registry key that is selected for addition to the list of protected resources.

The field is available when you add a registry key as a protected resource.

Browse

Clicking this button opens a window. In this window you can select a file or folder, registry key or network service, or create a list of IP addresses for addition to the list of protected resources.

Select file or folder window

In this window, the administrator can select a protected resource.

The following settings are available:

Object

Field that displays the path to the file or folder that is selected in the above folder tree.

You can also type the path to a file or folder manually.

Only file name masks with full paths to files can be entered. For example:

- C:\dir*. * or C:\dir* or C:\dir\ – All files in the C:\dir\ folder.
- C:\dir*.exe – All files with the .exe extension in the C:\dir\ folder.
- C:\dir*.ex? – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- C:\dir\test – Only the file C:\dir\test.

Select registry object window

In this window, the administrator can select a protected resource.

The following settings are available:

Key

Field that shows the path to the registry key that is selected in tree mentioned above. You can type the path to the key manually.

For example,

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
```

Value

Field that shows the value of the registry key that is selected in the above tree.

For example, the value for the key

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  
is Shell.
```

Category of protected resources window

In this window, the administrator can select a protected resource.

The following settings are available:

Category of protected resources

Field for entering the name of a category of resources access to which should be protected by Application Privilege Control.

Application Privilege Control adds the created category of protected resources to the current category. You can add both individual protected resources and other categories of protected resources to the newly created category of protected resources.

Application Activity Monitor tab

This table contains summary information about the activity of applications that are running in the operating system.

You can sort table contents by the contents of any of the columns. To do so, click the column header. Clicking the column header causes Kaspersky Endpoint Security to sort table contents by column contents in strict alphabetical order. Clicking the column header again causes Kaspersky Endpoint Security to sort table contents by column contents in reverse alphabetical order.

The table contains the following columns:

- **Application.** This column shows the name of the running application.
- **Process.** This column shows the name of the process that is generated by the running application.
- **KL category.** This column shows the name of the KL category to which Kaspersky Endpoint Security has assigned the running application.
- **Reputation.** This column shows the name of the trust group to which Kaspersky Endpoint Security or the user has assigned the running application. When the `Custom settings` line appears in this column, this means that the user has modified the settings of the application control rule.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Severity of vulnerability.** This column displays information about the severity of an application vulnerability:
 - **No vulnerabilities found.** No vulnerabilities are detected in the executable file of the running application.
 - **Critically vulnerable.** The running application contains a critical vulnerability that must be fixed immediately. Intruders actively exploit such vulnerabilities to infect computers.
 - **Dangerously vulnerable.** The running application contains a vulnerability that must be fixed soon. Analysis of currently available data indicates that intruders may start to actively exploit this vulnerability to infect the computer.

- **Possibly vulnerable.** The running application may contain a vulnerability, but fixing the vulnerability can be postponed. Analysis of currently available data indicates that intruders are not likely to actively exploit this vulnerability.
- **Web statistics.** This column shows allow and block statistics of running applications that attempt to access web resources. The statistics are shown in N1 \ N2 format, where N1 and N2 represent the number of allowed and blocked attempts, respectively.

If no data is available for this column (the control component corresponding to this column is disabled or has not been installed), the `Information is not available` line appears in this column.

Select trust group window

In this window, the administrator can select a trust group for applications started before Kaspersky Endpoint Security.

The following settings are available:

Trust groups. A table of trust groups for applications started before Kaspersky Endpoint Security

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups, depending on the level of threat that the applications pose to the operating system.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.



Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.




Inside each trust group, applications are combined into subgroups by vendor name. You can view subgroups by clicking the  icon to the left of the name of a group of applications. You can hide the list of subgroups by clicking the  icon to the left of the name of a group of applications.

The table contains the following columns:

- **Group.** This column shows trust groups and application groups.
- **Network.** This column shows the Firewall response on detecting network activity of an application group that is subject to a set of preset network rules. The Firewall response is designated by an icon that applies to the entire set of pre-configured network rules.

You can change the Firewall action for the entire set of preset network rules in the settings of the Firewall component. If you need to configure Firewall responses for individual network rules, you can do so on the **Network rules** tab of the **Application group control rules** window.

The Firewall action is marked using one of the following icons:

- The  icon signifies that Firewall allows a group of applications to access the network resource.
- The  icon signifies that Firewall blocks a group of applications from accessing the network resource.
- The  icon signifies that you have specified different Firewall responses for a set of preset network rules for an application group on the **Network rules** tab.

If the **Inherit** item has been selected in the context menu of an application group on the **Network rules** tab, the application group inherits the Firewall action from the parent group of applications. The icon is lighter in color than the icons of the parent group of applications.

Application Startup Control

This section contains information about Application Startup Control and instructions on how to configure the component settings.

In this section:

About Application Startup Control	84
Application Startup Control subsection	84

About Application Startup Control

The Application Startup Control component monitors user attempts to start applications and regulates the startup of applications by using *Application Startup Control rules*.

Startup of applications whose settings do not match any of the Application Startup Control rules is regulated by the selected operating mode of the component. *Black List mode* is selected by default. This mode allows any user to start any application.

All user attempts to start applications are logged in reports.

Application Startup Control subsection

In this window, the administrator can perform the following tasks:

- Enable and disable Application Startup Control.
- Select the Application Startup Control mode - **Black list** or **White list**.
- Create Application Startup Control rules.
- Enable and disable control of DLL modules and drivers.
- Form templates for messages about events that occurred during the operation of Application Startup Control.

- View the list of applications installed on the computer.

The following settings are available:

Enable Application Startup Control

This check box enables / disables the Application Startup Control component.

When the check box is selected, Kaspersky Endpoint Security controls user attempts to start applications.

When the check box is cleared, Kaspersky Endpoint Security does not control user attempts to start applications.

This check box is cleared by default.

Application Startup Control mode

Items in this drop-down list define the operating mode of Application Startup Control.

You can choose one of the following items:

- **Black List**

If this item is selected, Application Startup Control allows all users to start any applications, except in cases when applications satisfy the conditions of Application Startup Control block rules.

- **White List**

If this item is selected, Application Startup Control blocks all users from starting any applications, except in cases when applications satisfy the conditions of Application Startup Control allow rules.

When this mode is selected, two Application Startup Control rules are created automatically:

- **Golden Image.**
- **Trusted updaters.**

The settings of these rules cannot be edited. You cannot delete these rules. You can enable or disable these rules by selecting or clearing the check box opposite the relevant rule. By default, the Golden Image rule is enabled, and the Trusted Updaters rule is disabled. All users are allowed to start applications that match the trigger conditions of these rules.

The **Black List** option is selected by default.

Action

Items in this drop-down list define the action to be performed by the component when a user attempts to start an application that is blocked by Application Startup Control rules.

You can choose one of the following items:

- **Block**

If this item is selected, when the user attempts to start an application that is blocked in the current mode of Application Startup Control, Kaspersky Endpoint Security blocks this application from starting. Information about the blocked application startup is logged in the report.

- **Notify**

If this item is selected, Kaspersky Endpoint Security allows the startup of the application that is blocked in the current mode of Application Startup Control, but logs information about its startup in the report.

The default option is **Block**.

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of the **Rule name**, **Allowed**, or **Blocked** columns of the Application Startup Control rule that you want to find in the table.

To view the search results in sequence, use the ◀ and ▶ buttons.

Add

Clicking this button opens the **Application Startup Control rule** window. You can create a new rule in this window.

Edit

Clicking this button opens the **Application Startup Control rule** window. You can edit the settings of the selected rule in this window.

The button is available if a rule to edit is selected from the list of rules.

Delete

This button deletes the selected rule.

The button is available if a rule is selected from the list of rules.

Application Startup Control rules

Table with a list of Application Startup Control rules.

The table contains the following columns:

- **Status.** This column displays the operating status of the rule:
 - **On.** This status means that the rule is used when Application Startup Control is in operation.

The check box selected next to the rule corresponds to this status.

- **Off.** This status means that the rule is ignored when Application Startup Control is in operation.

The check box cleared next to the rule corresponds to this status.

- **Rule name.** This column displays the name of the rule.

- **Allowed.** This column displays the names of users and / or user groups that are allowed to start applications that match the rule parameters.
- **Blocked.** This column displays the names of users and / or user groups that are prohibited from starting applications that match the rule parameters.

Monitor DLL and drivers

This check box enables / disables additional control over the loading of DLL modules.

If the check box is selected, Kaspersky Endpoint Security controls the loading of DLL modules when users attempt to start applications. Information about the DLL module and the application that loaded this DLL module is logged in the report.

If the check box is cleared, Kaspersky Endpoint Security does not control the loading of DLL modules when users attempt to start applications.

This check box is cleared by default.

When monitoring DLL modules and drivers, it is not recommended to use Application Startup Control rules that were created based on KL categories. Determining KL categories (including in the “Operating system and its components” rules) for DLL modules and drivers may not work correctly. In particular, the “Operating system and its components” rule was created by default and is not distributed at DLL module and driver launch. When turning on this function, it is necessary to create separate allow rules for DLL modules and drivers. Using the Control DLL and drivers function if such allow rules do not exist could make the system unstable..

Templates

This button opens the **Message templates** window. In this window, you can edit the message templates. These messages appear on the screen when Application Startup Control rules are triggered.

Application list

Clicking this button opens the **List of applications** window. This window lets you view the list of all applications that have been started on the computer since the installation of Kaspersky Endpoint Security.

Blockage tab

The entry field contains the template of the message that is displayed when an Application Startup Control rule that blocks an application from starting is triggered.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

Clicking this button opens a drop-down list that lets you insert a variable in the template text.

The following items are possible:

- **Name of the rule that has been applied (%RULE%).** The variable is replaced with the name of the Application Startup Control rule that blocked the application from starting.
- **Current date (%DATE%).** The variable is replaced with the date on which the application was blocked from starting, in DD.MM.YYYY format.
- **Current time (%TIME%).** The variable is replaced with the time when the application was blocked from starting, in HH:MM format.
- **User name (%USER_NAME%).** The variable is replaced with the name of the current account on the computer on which the application was blocked from starting.
- **Computer name (%COMPUTER_NAME%).** The variable is replaced with the name of the computer on which the application was blocked from starting.
- **Name of the executable file on the drive (%FILE_NAME%).** The variable is replaced with the name of the executable file of the blocked application.
- **KL category of the executable file (%KL_CAT%).** The variable is replaced with the name of the KL category to which Kaspersky Endpoint Security assigns the blocked application.

- **Path to executable file (%FILE_PATH%).** The variable is replaced with the path to the executable file of the blocked application.
- **Executable file version (%FILE_VERSION%).** The variable is replaced with the version of the executable file of the blocked application.
- **Original name of the executable file (%ORIGINAL_FILE_NAME%).** The variable is replaced with the original name of the executable file of the blocked application.
- **Vendor (%FILE_PUBLISHER%).** The variable is replaced with the name of the vendor of the blocked application.
- **Application name (%FILE_PRODUCT_NAME%).** The variable is replaced with the name of the blocked application.
- **Hash of the executable file (%FILE_MD5%).** The variable is replaced with the MD5 hash code of the executable file of the blocked application.
- **Certificate issuer (%CERT_ISSUER%).** The variable is replaced with the name of the issuer of the blocked application certificate.
- **Certificate subject (%CERT_SUBJECT%).** The variable is replaced with the subject of the certificate of the blocked application.
- **Certificate thumbprint (%CERT_THUMBPRINT%).** The variable is replaced with the thumbprint of the certificate of the blocked application.

Link. Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Message to administrator tab

The entry field contains the template of the user's message that is sent to the LAN administrator if the user believes that application startup has been blocked by mistake.

You can edit the text of the template.

To

Field for entering the email addresses to which messages should be sent to the LAN administrator.

Subject

Field for entering the subject of the message to the administrator.

The default subject is [Application Startup Control] Mistaken blocking.

By default

This button restores the original text of the template.

Variable

Clicking this button opens a drop-down list that lets you insert a variable in the template text.

The following items are possible:

- **Name of the rule that has been applied (%RULE%).** The variable is replaced with the name of the Application Startup Control rule that blocked the application from starting.
- **Current date (%DATE%).** The variable is replaced with the date on which the application was blocked from starting, in DD.MM.YYYY format.
- **Current time (%TIME%).** The variable is replaced with the time when the application was blocked from starting, in HH:MM format.
- **User name (%USER_NAME%).** The variable is replaced with the name of the current account on the computer on which the application was blocked from starting.
- **Computer name (%COMPUTER_NAME%).** The variable is replaced with the name of the computer on which the application was blocked from starting.
- **Name of the executable file on the drive (%FILE_NAME%).** The variable is replaced with the name of the executable file of the blocked application.
- **KL category of the executable file (%KL_CAT%).** The variable is replaced with the name of the KL category to which Kaspersky Endpoint Security assigns the blocked application.
- **Path to executable file (%FILE_PATH%).** The variable is replaced with the path to the executable file of the blocked application.

- **Executable file version (%FILE_VERSION%).** The variable is replaced with the version of the executable file of the blocked application.
- **Original name of the executable file (%ORIGINAL_FILE_NAME%).** The variable is replaced with the original name of the executable file of the blocked application.
- **Vendor (%FILE_PUBLISHER%).** The variable is replaced with the name of the vendor of the blocked application.
- **Application name (%FILE_PRODUCT_NAME%).** The variable is replaced with the name of the blocked application.
- **Hash of the executable file (%FILE_MD5%).** The variable is replaced with the MD5 hash code of the executable file of the blocked application.
- **Certificate issuer (%CERT_ISSUER%).** The variable is replaced with the name of the issuer of the blocked application certificate.
- **Certificate subject (%CERT_SUBJECT%).** The variable is replaced with the subject of the certificate of the blocked application.
- **Certificate thumbprint (%CERT_THUMBPRINT%).** The variable is replaced with the thumbprint of the certificate of the blocked application.

The method used to send messages and the utilized template depends on whether or not there is an active Kaspersky Security Center policy running on the computer that has Kaspersky Endpoint Security installed, and whether or not there is a connection with the Kaspersky Security Center Administration Server. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Security Center installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Security Center installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage. The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.
 - If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.
 - If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.


Applications from registry window

In this window, the administrator can view a list of applications installed on the computer.

The following settings are available:

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of the **File**, **Vendor**, **Path**, **KL category** columns of the **Applications from registry** column. All table rows containing the characters that are entered in the search field are displayed in the table under the search field.

To reset the search results, delete the contents of the search field or click the  button in the search field.

Applications from registry. A table listing applications whose information is contained in the registry.

The table contains the following columns:

- **File.** This column shows the original name of the executable file of the application.
- **Vendor.** This column shows the name of the application vendor.
- **Path.** This column shows the path to the executable file of the application.
- **KL category.** This column shows the name of the KL category to which an application belongs.

Application Startup Control rule window

In this window, the administrator can create Application Startup Control rules.

An Application Startup Control rule specifies the triggering conditions and the action performed by Application Startup Control when the rule is triggered (allowing or blocking application startup by users).

Rules use inclusion and exclusion conditions:

- *Inclusion conditions.* Kaspersky Endpoint Security applies the rule to the application if the application matches at least one of the inclusion conditions.
- *Exclusion conditions.* Kaspersky Endpoint Security does not apply the rule to the application if the application matches at least one of the exclusion conditions and does not match any of the inclusion conditions.

The administrator can perform the following actions on Application Startup Control rules:

- Add a new rule
- Create or change the conditions for the triggering of a rule
- Edit rule status

An Application Startup Control rule can be enabled (the check box opposite the rule is selected) or disabled (the check box opposite the rule is cleared). An Application Startup Control rule is enabled by default after it is created.

- Delete rule

To work with Application Startup Control rules, the following settings are available:

Rule name


Field for entering the name of the Application Startup Control rule.

Description

This field lets you describe an application or group of applications for which an Application Startup Control rule has been defined.

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of the **Condition criterion** or **Condition value** columns from the **Inclusion conditions / Exclusion conditions** table. All trigger conditions for Application Startup Control rules for applications that match the search criteria are listed in the **Inclusion conditions / Exclusion conditions** table.

To reset the search results, delete the contents of the search field or click the  button in the search field.

Inclusion conditions / Exclusion conditions

This table lists inclusion / exclusion conditions that trigger an Application Startup Control rule.

The table contains the following columns:

- **Condition criterion.** This column shows the criterion of a condition that triggers the rule. Clicking the **Add** button displays the list of available criteria.
- **Condition value.** This column shows the value of the condition that triggers a rule. For example: the path to the executable file of the application, metadata, or type of drive that stores the file.

Add

This button opens the button context menu with the following items:

- **Condition(s) from properties of files in the specified folder.** Selecting this item opens the **Select folder** window. This window lets you select a folder that contains the executable files of applications. One or several rule triggering conditions are formed from the properties of executable files.
- **Condition(s) from properties of started applications.** Selecting this item opens the **Add condition** window. This window lets you create a rule-triggering condition that is based on the properties of applications that are running on the computer.
- **Condition(s) "KL category".** Selecting this item opens the **Condition(s) "KL category"** window. This window lets you select one or more KL application categories based on which one or more rule-triggering conditions will be created.
- **Custom condition.** Selecting this item opens the **Custom condition** window. You can manually create the condition that triggers the rule in this window.
- **Condition by file drive.** Selecting this item opens the **Condition by file drive** window. This window lets you create a condition that triggers an rule based on information about the drive where the executable file of an application is stored.

Edit

Clicking this button opens a window with the settings of the rule-triggering condition that is selected in the Inclusion conditions or Exclusion conditions table. You can edit the condition that triggers the rule in this window.

This button is available when a rule-triggering condition is selected in the **Inclusion conditions / Exclusion conditions** table.

Delete

Clicking this button deletes the rule-triggering condition that is selected in the **Inclusion conditions / Exclusion conditions** table.

This button is available when a rule-triggering condition is selected in the **Inclusion conditions / Exclusion conditions** table.

Convert to exclusion

Clicking this button converts an inclusion condition that is selected in the **Inclusion conditions** table into an exclusion condition and moves it to the **Exclusion conditions** table.

Convert to inclusion condition

Clicking this button converts an exclusion condition that is selected in the **Exclusion conditions** table into an inclusion condition and moves it to the **Inclusion conditions** table.

Principals and their rights

This table lets you specify users and/or user groups covered by the Application Startup Control rule.

The table contains the following columns:

- **Subject.** This column shows the users and/or user groups covered by the Application Startup Control rule.

The **Everyone** group is added by default. The rule applies to all users of a given computer.

- **Allow.** This column shows a check box that enables / disables permission to start applications that satisfy the rule conditions for users and/or user groups specified in the **Subject** column.

By default, the check box is cleared when the component runs in **Black list** mode and selected when the component runs in **White list** mode.

- **Deny.** This column shows a check box that enables / disables prohibition to start applications that satisfy the rule conditions for users and/or user groups specified in the **Subject** column.

By default, the check box is selected when the component runs in **Black list** mode and cleared when the component runs in **White list** mode.

Add

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window you can select the users and/or groups of users to be covered by the rule.

Delete

Clicking this button removes the selected user and/or user group from the **Principals and their rights** table. The component stops monitoring the startup of applications that satisfy the rule conditions by these users.

Deny for other users

If this check box is selected, the application blocks all users that do not appear in the **Principals and their rights** table from starting applications that satisfy the rule conditions.

If this check box is cleared, the application allows only users that appear in the table or belong to user groups appearing in the table to start applications that satisfy the rule conditions.

This check box is cleared by default.

Trusted updaters

The check box enables / disables the startup of applications which have been installed or updated by applications from the category that is specified in the rule, and for which no blocking rules are defined.

If the check box is selected, Kaspersky Endpoint Security considers applications that belong to the category that is specified in the rule to be trusted. Kaspersky Endpoint Security allows the startup of applications which have been installed or updated by applications from the category that is specified in the rule if no blocking rules are defined for them.

By default, the check box is not selected.

Add condition window

In this window, the administrator can add a triggering condition to a created rule.

Rule-triggering conditions are created using criteria. The following criteria are used to create rules in Kaspersky Endpoint Security:

- Path to the folder containing the executable file of the application or path to the executable file of the application.
- Metadata: application executable file name, application executable file version, application name, application version, application vendor.
- Hash of the executable file of the application.

- Certificate: issuer, principal, thumbprint.
- Inclusion of the application in a KL category.
- Location of the application executable file on a removable drive.

The criterion value must be specified for each criterion used in the condition. If the parameters of the application being started match the values of criteria specified in the inclusion condition, the rule is triggered. In this case, Application Startup Control performs the action prescribed in the rule. If application parameters match the values of criteria specified in the exclusion condition, Application Startup Control does not control startup of the application.

To add a rule triggering condition, the following settings are available:

Folder

A field that shows the path to the folder that contains the executable files of applications. The details of executable files of applications are shown in the table below.

Select

This button opens the **Select folder** window. This window lets you select a folder that contains the executable files of applications. The details of executable files of applications are shown in the table below.

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of columns in the table that contains information on the executable files of applications. The first entry that matches the characters that are typed in the search field is highlighted in gray in the table.

To reset the search results, click the  button in the search field.

Show criterion

A drop-down list whose items determine the contents of the table with information on the executable files of applications:

- **File hash code.** If this item is selected, the table contains the original names of executable files of applications and hashes of executable files of applications.

- **Certificate.** If this item is selected, the table contains the original names of executable files of applications and certificate details (issuer, subject, thumbprint).

If this item is selected, the **Use data** section becomes available.

- **KL category.** If this item is selected, the table contains the original names of the executable files and the names of the KL categories to which those applications belong.
- **Metadata.** If this item is selected, the table contains metadata (original names of executable files of applications, names of executable files on the drive, versions of executable files, names of applications, and names of application vendors).

If this item is selected, the **Use data** section becomes available.

- **Folder path.** If this item is selected, the table contains the original names of executable files of applications and paths to folders with executable files of applications.

Issuer

This check box enables / disables the use of the application certificate issuer in the rule triggering condition.

This check box is cleared by default.

This check box is displayed when the **Certificate** item is selected in the **Show criterion** drop-down list.

Subject

This check box enables / disables the use of the application certificate subject in the rule triggering condition.

This check box is cleared by default.

This check box is displayed when the **Certificate** item is selected in the **Show criterion** drop-down list.

Thumbprint

This check box enables / disables the use of the application certificate thumbprint in the rule triggering condition.

This check box is selected by default.

This check box is displayed when the **Certificate** item is selected in the **Show criterion** drop-down list.

File name

This check box includes / excludes the original name of the executable file of an application from the rule-triggering condition.

When the check box is selected, the original name of the executable file of an application is included in the rule-triggering condition.

This check box is cleared by default.

This check box is displayed when the **Metadata** item is selected in the **Show criterion** drop-down list.

File version

This check box includes / excludes version information of the executable file of an application from the rule-triggering condition.

When the check box is selected, the version of the executable file is included in the rule-triggering condition.

This check box is cleared by default.

This check box is displayed when the **Metadata** item is selected in the **Show criterion** drop-down list.

Application name

This check box includes / excludes information about the application name from the rule-triggering condition.

When the check box is selected, the application name is included in the rule-triggering condition.

This check box is cleared by default.

This check box is displayed when the **Metadata** item is selected in the **Show criterion** drop-down list.

Application version

This check box includes / excludes application version information from the rule-triggering condition.

When the check box is selected, the application version is included in the rule-triggering condition.

This check box is cleared by default.

This check box is displayed when the **Metadata** item is selected in the **Show criterion** list.

Vendor

This check box includes / excludes information about the application vendor from the rule-triggering condition.

When the check box is selected, the application vendor name is included in the rule-triggering condition.

This check box is cleared by default.

This check box is displayed when the **Metadata** item is selected in the **Show criterion** drop-down list.

Executable files of applications. This table contains information on the executable files of applications.

Depending on the item that is selected in the **Show criterion** drop-down list, the table may contain different columns.

If the **File hash code** item is selected in the **Show criterion** drop-down list, the table contains the following columns:

- **File.** This column shows the name and extension of the executable file of an application.

The check box opposite the name of the executable file includes / excludes information about the executable file of an application from the condition that triggers the Application Startup Control rule.

- **File hash code.** This column shows the SHA256 hash code of the executable file of an application.

If the **Certificate** item is selected in the **Show criterion** drop-down list, the table contains the following columns:

- **File.** This column shows the name and extension of the executable file of an application.

The check box opposite the name of the executable file includes / excludes information about the executable file of an application from the condition that triggers the Application Startup Control rule.

- **Issuer.** This column shows the name of the application certificate issuer.
- **Subject.** This column shows the private or corporate name of the application certificate subject.
- **Thumbprint.** This column shows the thumbprint of the application certificate.

If the **KL category** item is selected in the **Show criterion** drop-down list, the table contains the following columns:

- **File.** This column shows the name and extension of the executable file of an application.

The check box opposite the name of the executable file includes / excludes information about the executable file of an application from the condition that triggers the Application Startup Control rule.

- **KL category.** This column shows the KL category to which Kaspersky Endpoint Security assigns an application.

If the **Metadata** item is selected in the **Show criterion** drop-down list, the table contains the following columns:

- **File.** This column shows the name and extension of the executable file of an application.

The check box opposite the name of the executable file includes / excludes information about the executable file of an application from the condition that triggers the Application Startup Control rule.

- **File name.** This column shows the name of the executable file of an application.
- **File version.** This column shows the version of the executable file of an application.
- **Application name.** This column shows the application name.
- **Application version.** This column shows the application version.

- **Vendor.** This column shows the name of the vendor of the executable file of an application.

If the **Folder path** item is selected in the **Show criterion** drop-down list, the table contains the following columns:

- **File.** This column shows the name and extension of the executable file of an application.

The check box opposite the name of the executable file includes / excludes information about the executable file of an application from the condition that triggers the Application Startup Control rule.

- **Folder path.** This column shows the path to the folder that contains the executable file of an application.

You can sort table contents by the contents of any of the columns. To do so, click the column header. Clicking the column header causes Kaspersky Endpoint Security to sort table contents by column contents in reverse alphabetical order. Clicking the column header again causes Kaspersky Endpoint Security to sort table contents by column contents in strict alphabetical order.

Custom condition window

In this window, the administrator can add a triggering condition to a created rule.

Rule-triggering conditions are created using criteria. The following criteria are used to create rules in Kaspersky Endpoint Security:

- Path to the folder containing the executable file of the application or path to the executable file of the application.
- Metadata: application executable file name, application executable file version, application name, application version, application vendor.
- Hash of the executable file of the application.
- Certificate: issuer, principal, thumbprint.
- Inclusion of the application in a KL category.
- Location of the application executable file on a removable drive.

The criterion value must be specified for each criterion used in the condition. If the parameters of the application being started match the values of criteria specified in the inclusion condition, the rule is triggered. In this case, Application Startup Control performs the action prescribed in the rule. If application parameters match the values of criteria specified in the exclusion condition, Application Startup Control does not control startup of the application.

To add a rule triggering condition, the following settings are available:

Select

Clicking this button opens the standard **Open** window in Microsoft Windows. This window lets you select an application executable file, whose properties then populate the fields of the **Custom condition** window. The path to the selected executable file is shown in the field on the left.

File hash code

If this option is selected, the rule-triggering condition is created on the basis of the SHA256 hash of the executable file of an application.

Kaspersky Endpoint Security does not support MD5 hash code.

You can edit the contents of the field corresponding to the **File hash code** option.

Certificate

If this option is selected, the rule-triggering condition is created on the basis of application certificate data.

Issuer

This check box enables / disables the use of the certificate issuer in the rule triggering condition.

The certificate issuer is displayed in the field to the right of the **Issuer** check box. Specify the complete unique name of the issuer. The characters used in the name are not case-sensitive.

You can use wildcards: "*" for any number of random symbols and "?" for one random symbol.

This check box is cleared by default.

The check box is available when the **Certificate** option is selected.

Subject

This check box enables / disables the use of the certificate subject in the rule triggering condition.

The certificate subject is displayed in the field to the right of the **Subject** check box. Specify the complete unique name of the subject. The characters used in the name are not case-sensitive.

You can use wildcards: "*" for any number of random symbols and "?" for one random symbol.

This check box is cleared by default.

The check box is available when the **Certificate** option is selected.

Thumbprint

This check box enables / disables the use of the certificate thumbprint in the rule triggering condition.

The certificate thumbprint is displayed in the field to the right of the **Thumbprint** check box. You can edit the field contents.

This check box is selected by default.

The check box is available when the **Certificate** option is selected.

Metadata

If this option is selected, the rule-triggering condition is created on the basis of the metadata of the executable file of an application.

By default, this option is selected.

File name

This check box includes / excludes the name of the executable file of an application from the rule-triggering condition.

When the check box is selected, the name of the executable file of an application is included in the rule-triggering condition.

The name of the executable file of an application is shown in the field on the right of the **File name** check box. You can edit the field contents.

This check box is cleared by default.

The check box is available when the **Metadata** option is selected.

File version

This check box includes / excludes version information of the executable file of an application from the rule-triggering condition.

When the check box is selected, the version of the executable file is included in the rule-triggering condition.

This check box is cleared by default.

The check box is available when the **Metadata** option is selected.

Equal to / Not equal to / Similar to / Contains / Begins with / Ends with / More than / More than or equal to / Less than / Less than or equal to

A drop-down list whose values specify the version of the executable file of an application / application version in the rule-triggering condition. The following list items are available:

- **Equal to.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers are equal to the version number that is entered in the field on the right of the drop-down list.
- **Not equal to.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers are not equal to the version number that is entered in the field on the right of the drop-down list.
- **Similar to.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers contain the characters that are entered in the field on the right of the drop-down list. You can enter the version number by using wildcards:
 - * – Represents a sequence of any zero or more characters.
 - ? – Represents any single character.
- **Contains.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers contain the characters that are entered in the field on the right of the drop-down list.

- **Begins with.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers begin with the characters that are entered in the field on the right of the drop-down list.
- **Ends with.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers end with the characters that are entered in the field on the right of the drop-down list.
- **More than.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers are higher than the version number that is entered in the field on the right of the drop-down list.

For one application version number to be higher than another application version number, one or more of the digits in the first application version must be higher than the corresponding digits in the other application version.

- **More than or equal to.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers are higher than or equal to the version number that is entered in the field on the right of the drop-down list.
- **Less than.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers are lower than the version number that is entered in the field on the right of the drop-down list.

For one application version number to be lower than another application version number, one or more of the digits in the first application version must be lower than the corresponding digits in the other application version.

- **Less than or equal to.** When this item is selected, the rule-triggering condition is satisfied by applications whose version numbers are lower than or equal to the version number that is entered in the field on the right of the drop-down list.

The drop-down list is available when the **File version** or **Application version** check box is selected.

Application name

This check box includes / excludes information about the application name from the rule-triggering condition.

When the check box is selected, the application name is included in the rule-triggering condition.

This check box is cleared by default.

The check box is available when the **Metadata** option is selected.

Application version

This check box includes / excludes application version information from the rule-triggering condition.

When the check box is selected, the application version is included in the rule-triggering condition.

This check box is cleared by default.

The check box is available when the **Metadata** option is selected.

Vendor

This check box includes / excludes information about the application vendor from the rule-triggering condition.

When the check box is selected, the application vendor name is included in the rule-triggering condition.

This check box is cleared by default.

The check box is available when the **Metadata** option is selected.

File or folder path

If this option is selected, the rule-triggering condition is created on the basis of the specified path to a file or folder.

You can edit the contents of the field corresponding to the **Path to file or folder** option.

Resolve symbolic link

Clicking this button causes Kaspersky Endpoint Security to resolve the symbolic link indicated in the **Path to file or folder** field. The symbolic link is replaced by the full path to the file to which the link is directed.

The button is available if the specified path leads to the symbolic link.

Select file

Clicking this button opens the standard **Open** window in Microsoft Windows. This window lets you select the executable application file. The file to the executable file of the application is shown in the field on the left of the **Select file** button. You can also modify the path to the executable file manually.

Select folder

This button opens the **Select folder** window. This window lets you select the folder with the executable file based on which you want to create a condition that triggers an Application Startup Control rule. The path to the folder is shown in the field on the left of the **Select** button. You can also manually edit the path to the folder that contains the executable file.

Condition by file drive window

In this window, the administrator can select the location of an application's executable file on a removable drive as a rule triggering condition.

The following setting is available:

Drive

A drop-down list that lets you select the type of drive that stores the executable files of applications, based on which a condition that triggers the rule is created.

Possible value of the drop-down list: **Removable drive**. If this item is selected, the rule controls the launch of executable files that are stored on removable drives.


Condition(s) "KL category" window

In this window, the administrator can select the KL category as a rule triggering condition.

The following settings are available:

Search field

In the search field, you can enter the full name or several characters from the name of the KL category that you want to find in the list of **KL categories**. The first KL category that matches the characters that are entered in the search field is highlighted in gray.

To reset the search results, delete the contents of the search field or click the  button in the search field.

KL categories

A KL category is a list of applications that have shared theme attributes. The list is maintained by Kaspersky Lab specialists. Check boxes opposite the names of KL categories include / exclude KL categories from the rule triggering conditions.

When the check box opposite the name of a KL category is selected, a condition that triggers a rule is created on the basis of this KL category.

Device Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Device Control and instructions on how to configure the component settings.

In this section:

About Device Control	112
Device Control subsection.....	113

About Device Control

Device Control ensures the security of confidential data by restricting user access to devices that are installed on the computer or connected to it, including:

- Data storage devices (hard drives, removable drives, tape drives, CD/DVD drives)
- Data transfer tools (modems, external network cards)
- Devices that are designed for converting data to hard copies (printers)
- Connection buses (also referred to as simply "buses"), referring to interfaces for connecting devices to computers (such as USB, FireWire, and Infrared)

Device Control manages user access to devices by applying *device access rules* (also referred to as "access rules") and *connection bus access rules* (also referred to as "bus access rules").

Device Control subsection

In this window, the administrator can perform the following tasks:

- Enable and disable Device Control.
- Form templates for messages about events that occurred during the operation of Device Control.
- Configure rules for user access to computer devices.
- Configure the logging of information about operations with files on removable drives.
- Configure connection bus access rules.
- Create a list of trusted devices.

The following settings are available:

Enable Device Control

This check box enables / disables the Device Control component.

If the check box is selected, Kaspersky Endpoint Security uses access rules to control access to devices that are connected to the computer.

If the check box is cleared, Kaspersky Endpoint Security does not control access to all devices, so that all users are granted access to all devices that are connected to the computer.

This check box is selected by default.

Device types

The tab displays a table containing all possible types of devices according to the classification of the Device Control component, including their respective access statuses.

The table contains the following columns:

- **Devices.** This column displays the names of the types of devices.

You can sort the list of device access rules by the names of the types of devices. To do this, click the header of the **Devices** column.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of device access rules in reverse alphabetical order. After you click the header of the column for the second time, Kaspersky Endpoint Security sorts the list of device access rules in strict alphabetical order.

- **Access.** This column displays the status of access to the types of devices (*Allow*, *Block*, *Depends on bus*, *Allowed with restrictions*).

A rule is assigned *Allowed with restrictions* status if its status had been *Allowed* and you have changed the rule settings.

Edit

This button opens the **Configuring device access rule** window. You can edit the settings of an access rule in this window.

The button is only available for the access rules for device types which have a file system.

Logging

Clicking this button opens the **Logging Settings** window. This window lets you enable or disable logging of information about operations with files on removable drives. You can also specify an event filter based on file formats or specify users information about whose actions will be logged.

This button is available only for removable drive access rules.

Connection buses

This tab displays a table with a list of all available connection buses according to the Device Control component's classification, including their respective access statuses:

- **Device connection buses.** This column displays the names of the connection buses.

You can sort the list of connection bus access rules by the names of the buses. To do this, click the header of the **Device connection buses** column.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of bus access rules in reverse alphabetical order. After you click the header of the column for the second time, Kaspersky Endpoint Security sorts the list of bus access rules in strict alphabetical order.

- **Access.** This column displays the statuses of access to the connection buses (*Allow*, *Block*).

Trusted devices

The tab shows a table with the following data:

- **Name.** This column displays the names of the trusted devices.
- **Users.** This column displays the names of the users and / or groups of users who are always granted full access to devices.
- **Comment.** The column shows information about trusted devices that was entered while devices were being added to the Trusted list.
- **Device model / ID.** This column displays the models and / or IDs of trusted devices.
- **Device type.** This column displays the type of a particular device.

You can sort the list of trusted devices by any of the table columns. To do so, left-click the column header.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of trusted devices in reverse alphabetical order. After you click the header of the column for the second time, Kaspersky Endpoint Security sorts the list of trusted devices in strict alphabetical order.

You can change the composition of table columns. To do so, right-click the header of any table column, and in the context menu that opens clear / select check boxes opposite the names of columns that you want to exclude from / include in the table.

You can rearrange the table columns. To do so, left-click a column header and drag it to a new location.

Select

This button opens the **Select trusted devices** window. In this window, you can select one or several devices to add to the list of trusted devices, edit the list of trusted devices, and change the user and/or user group for whom such devices are trusted.

Edit

This button opens the **Configuring device access rule** window for a trusted device. In this window, you can change the user and / or group of users for which the device is specified as trusted.

This button is available if a trusted device is selected from the list of trusted devices.

Delete

This button deletes the selected trusted device from the list of trusted devices.

If the device has been deleted from the list of trusted devices, a decision on access to the device is made based on the access rule that is applied to this device type.

This button is available if a trusted device is selected from the list of trusted devices.

Templates

This button opens the **Templates** window. In this window, you can edit the template of the message which is displayed when the user attempts to access a blocked device, and the template of the complaint message that is sent to the LAN administrator.

Blockage tab

The entry field contains the template of the message that is displayed when the user attempts to access a blocked device or to perform a forbidden operation with device content.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **Current date (%DATE%)**. This variable is replaced with the date when access to the device is blocked or an operation with the device content is forbidden.
- **Current time (%TIME%)**. This variable is replaced with the time when access to the device is blocked or an operation with the device content is forbidden.

- **User name (%USER_NAME%).** This variable is replaced with the name of the current user account that has been blocked from an operation with device content.
- **Computer name (%COMPUTER_NAME%).** This variable is replaced with the name of the computer on which access to the device is blocked or an operation with the device content is forbidden.
- **Device type (%DEVICE_TYPE%).** This variable is replaced with the name of the device type to which access is blocked or an operation with the content of which is forbidden.
- **Device name (%DEVICE_NAME%).** This variable is replaced with the name of the device to which access is blocked or an operation with the content of which is forbidden.
- **Operation (%OPERATION%).** This variable is replaced with the name of the type of blocked operation with device content.
- **Device ID (%DEVICE_ID%).** This variable is replaced with the unique identifier of the device to which access is blocked or an operation with the content of which is forbidden.
- **Device model (%DEVICE_VIDPID%).** This variable is replaced with a string that contains the VID and PID of the device to which access is blocked or an operation with the content of which is forbidden.

Link

Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Insert link window

In this window, the administrator can specify the link that will be used in the text of the message template.

The following settings are available:

Web address

Use this field to specify the address of the web resource that opens via the link. This link is added to the text of the message template.

Link text

This field lets you specify the text of the link included in the message. Clicking this text in the message takes you to the web resource whose address is specified in the **Web address** field.

This field is optional. If this field is left blank, the web address of the link is inserted in the message template.

Preview

This field shows the preview of the link in the text of the message template.

Message to administrator tab

The entry field contains a template of the message that is sent to the LAN administrator when the user believes that access to the device is blocked or an operation with device content is forbidden by mistake.

You can edit the text of the template.

To

Field for entering the email address of the LAN administrator.

Subject

Field for entering the subject of the complaint message.

The default subject is `[DeviceControl] Mistaken blocking`.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **Current date (%DATE%).** This variable is replaced with the date when access to the device is blocked or an operation with the device content is forbidden.
- **Current time (%TIME%).** This variable is replaced with the time when access to the device is blocked or an operation with the device content is forbidden.

- **User name (%USER_NAME%).** This variable is replaced with the name of the current user account that has been blocked from an operation with device content.
- **Computer name (%COMPUTER_NAME%).** This variable is replaced with the name of the computer on which access to the device is blocked or an operation with the device content is forbidden.
- **Device type (%DEVICE_TYPE%).** This variable is replaced with the name of the device type to which access is blocked or an operation with the content of which is forbidden.
- **Device name (%DEVICE_NAME%).** This variable is replaced with the name of the device to which access is blocked or an operation with the content of which is forbidden.
- **Operation (%OPERATION%).** This variable is replaced with the name of the type of blocked operation with device content.
- **Device ID (%DEVICE_ID%).** This variable is replaced with the unique identifier of the device to which access is blocked or an operation with the content of which is forbidden.
- **Device model (%DEVICE_VIDPID%).** This variable is replaced with a string that contains the VID and PID of the device to which access is blocked or an operation with the content of which is forbidden.

The method used to send messages and the choice of template depends on whether or not there is an active Kaspersky Security Center policy running on the computer with Kaspersky Endpoint Security installed. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Security Center installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Security Center installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage. The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.
 - If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.
 - If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

Configuring device access rule window

In this window, the administrator can configure the settings of a device access rule.

A device access rule is a combination of parameters that define the following functions of the Device Control component:

- Allowing selected users and / or user group to access specific types of devices during specific periods of time.

You can select a user and / or user group and create a device access schedule for them.

- Setting the right to read the content of memory devices.
- Setting the right to edit the content of memory devices.

By default, access rules are created for all types of devices in the classification of the Device Control component. Such rules grant all users full access to the devices at all times, if access to the connection buses of the respective types of devices is allowed.

To configure access rules, the following settings are available:

Users and / or groups of users

The list contains users and / or groups of users for which the device access rule is configured.

Add

Button which opens the **Select Users or Groups** window in Microsoft Windows. In this window you can select a user and / or group of users for which you want to configure the device access rule.

Edit

Button which opens the **Select Users or Groups** window in Microsoft Windows. In this window, you can change the user and / or group of users for whom you want to configure the device access rule.

This button is available if the entry with the name of the user and / or group of users is selected from the **Users and / or groups of users** list.

Delete

This button deletes the user and / or group of users from the settings of the device access rule.

This button is available if the entry with the name of the user and / or group of users is selected from the **Users and / or groups of users** list.

Rights of the selected group of users by access schedules

This table provides information about restrictions on access to devices: list of device access schedules and a corresponding list of operations that the selected user and / or group of users can perform with devices.

The table contains the following columns:

- **Access schedule.** This column displays the name of a device access schedule. This check box enables / disables the use of a device access schedule for users and / or groups of users that are selected from the **Users and / or groups of users** list.

For a single item on the **Users and / or groups of users** list, you can select multiple device access schedules.

- **Read.** This column shows a check box that determines the right to read the content of devices for the time intervals that are specified in the access schedule when device access is granted:
 - If you want to allow users to view the content of the devices with access controlled by the access rule that you are configuring, select the check box next to the required device access schedule in the **Read** column.
 - If you want to prohibit users to view the content of the devices with access controlled by the access rule that you are configuring, clear the check box next to the required device access schedule in the **Read** column.
- **Write.** This column shows a check box that determines the right to write the content of devices for the time intervals that are specified in the access schedule when device access is granted:
 - If you want to allow users to change the content of the devices to which access is controlled by the access rule that you are configuring, select the check box next to the required device access schedule in the **Write** column.
 - If you want to forbid users to change the content of the devices to which access is controlled by the access rule that you are configuring, clear the check box next to the required device access schedule in the **Write** column.

Create

This button opens the **Schedule for access to devices** window. In this window, you can configure the schedule for device access on specified days of the week. The device access schedule is applied to users and / or groups of users that are selected in the **Users and / or groups of users** list.

Edit

This button opens the **Schedule for access to devices** window. In this window, you can edit a device access schedule for users and / or groups of users that are selected in the **Users and / or groups of users** list.

The button is available if a device access schedule, other than the default one, is selected from the **Rights of the selected group of users by access schedules** table.

Copy

This button copies the device access schedule that is selected from the **Rights of the selected group of users by access schedules** table.

The button is available if a device access schedule is selected from the **Rights of the selected group of users by access schedules** table.

Delete

This button deletes the selected device access schedule from the table.

The button is available if a device access schedule, other than the default one, is selected from the **Rights of the selected group of users by access schedules** table.

Schedule for access to devices window

In this window, you can configure the schedule for device access on specified days of the week. To do so, specify one or several time periods during which access to devices is monitored, for each day of the week.

Name

Field for entering the name of a device access schedule.

Schedule for access to devices

A device access schedule can be configured by using a special table. Table lines designate days of the week; table columns designate one-hour intervals in the time scale. Depending on the regional settings of the operating system, the time scale may be 24-hour or 12-hour.

The colors of table cells reflect the restrictions that are imposed:

- The gray color signifies that access to devices is not controlled by the device access rule.
- The green color signifies that access to the devices is controlled by the device access rule.

To add a time period to the device access schedule during which access to the device is not monitored, click the cells in the table that correspond to the relevant time and day of the week. The color of the cells turns gray.

To change the time period in the device access schedule during which access to the device is not monitored to a time period during which access to the device is monitored, click the gray cells in the table that correspond to the relevant time and day of the week. The color of the cells turns green.

Logging Settings window

In this window, the administrator can configure the settings for logging events associated with files on removable drives.

The following settings are available:

Enable logging

This check box enables / disables logging of information about operations with files on removable drives.

If the check box is selected, Kaspersky Endpoint Security logs information about write and removal operations performed with files on removable drives and sends a notification to the Kaspersky Security Center Administration Server.

If the check box is cleared, information about operations performed with files on removable drives is not logged anywhere.

This check box is cleared by default.

Write

This check box enables / disables logging of information about write to file operations on removable drives.

If the check box is selected, Kaspersky Endpoint Security logs information about write to file operations on removable drives and sends a notification to the Kaspersky Security Center Administration Server.

If the check box is cleared, information about write to file operations on removable drives is not saved anywhere.

This check box is selected by default.

The check box is available if the **Enable logging** check box is selected.

Delete

This check box enables / disables logging of information about file deletion on removable drives.

If the check box is selected, Kaspersky Endpoint Security logs information about file deletion on removable drives and sends a notification to the Kaspersky Security Center Administration Server.

If the check box is cleared, information about file deletion on removable drives is not saved anywhere.

This check box is cleared by default.

The check box is available if the **Enable logging** check box is selected.

Save information about all files

This check box enables / disables logging of all events.

If the check box is selected, Kaspersky Endpoint Security logs and sends to the Administration Server information about operations performed with all files on removable drives.

If the check box is cleared, Kaspersky Endpoint Security logs and sends to the Administration Server information about operations with files of those formats next to which a check box is selected in the **Filter on file formats** section.

This check box is cleared by default.

Filter on file formats

A list of file formats in connection with which Kaspersky Endpoint Security generates events to be logged and sent to the Administration Server. Each item in the list is a check box.

If the check box next to a file format is selected, Kaspersky Endpoint Security logs and sends to the Administration Server information about operations performed with files of the specified format.

The list includes the following file formats:

- **Text files**
- **Video files**
- **Audio files**
- **Graphic files**
- **Executable files**
- **Office files**
- **Database files**
- **Archives**

By default, check boxes are selected next to the following formats:

- **Text files**
- **Office files**
- **Database files**
- **Archives**

Items in the list are available when the **Save information about all files** check box is cleared.

Users

An entry field for specifying the names of users and / or groups.

When the users specified in this field write to files located on removable drives or delete files from removable drives, Kaspersky Endpoint Security logs the event and sends a message to the Kaspersky Security Center Administration Server.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. This window lets you select users and/or user groups information about whose actions will be logged by Kaspersky Endpoint Security and sent to the Administration Server.

Trusted Wi-Fi networks window

In this window, the administrator can form a list of trusted Wi-Fi networks.

The following settings are available:

Add

Clicking this button opens the **Trusted Wi-Fi network** window. This window lets you specify the settings of the rule according to which a Wi-Fi network is assigned to the trusted group.

Edit

Clicking this button opens the **Trusted Wi-Fi network** window. This window lets you edit the settings of the rule according to which a Wi-Fi network is assigned to the trusted group.

This button is available when a Wi-Fi network is selected in the table.

Delete

Clicking this button removes the selected Wi-Fi network from the list of trusted Wi-Fi networks.

If a Wi-Fi network has been removed from the list of Wi-Fi networks, the connection to this Wi-Fi network is denied in **Block with exceptions** mode.

This button is available when a Wi-Fi network is selected in the table.

Trusted Wi-Fi networks. This table contains information about trusted Wi-Fi networks. In **Block with exceptions** mode, the connection to Wi-Fi networks appearing in this list is allowed.

The table contains the following columns:

- **Network name.** This column shows the name of the Wi-Fi network. The Wi-Fi network with this name is considered trusted. Users are allowed to connect to this Wi-Fi network in **Block with exceptions** operating mode.

- **Authentication type.** This column shows the type of authentication used when connecting to the Wi-Fi network. Wi-Fi networks that use this type of authentication are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** operating mode.
- **Encryption type.** This column shows the type of encryption used to protect Wi-Fi network traffic. Wi-Fi networks that use this type of encryption are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** operating mode.
- **Comment.** This column shows additional information about the rule according to which a Wi-Fi network is assigned to the trusted group.

Trusted Wi-Fi network window

In this window, the administrator can configure the settings that determine which Wi-Fi networks must be considered trusted.

The following settings are available:

Network name

An entry field in which you can specify the name of the Wi-Fi network. The Wi-Fi network with this name is considered trusted. Users are allowed to connect to this Wi-Fi network in **Block with exceptions** mode.

Authentication type

Items in this drop-down list define the type of authentication upon the connection to a Wi-Fi network. Wi-Fi networks that use the specified type of authentication are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** mode.

The following items are available from the **Authentication type** drop-down list:

- **Any.**

If this item is selected, the type of authentication is not considered when determining whether or not a Wi-Fi network belongs to the trusted group.
- **No authentication.**

If this item is selected, Wi-Fi networks that do not require user authentication upon connection are considered trusted.

- **Specified key.**

If this item is selected, the specified key is used for authentication. The specified key corresponds to a specific "sender - recipient" pair.

- **WPA-Enterprise.**

If this item is selected, an extensible authentication protocol for corporate Wi-Fi networks is used. The user must have a certificate authorizing the user to access the Wi-Fi network. To receive this certificate, the user is verified against the database of registered users.

- **WPA-Personal.**

If this item is selected, an extensible authentication protocol for personal Wi-Fi networks is used. A password is set on a wireless router or access point. This password applies to all users.

- **WPA2-Enterprise.**

If this item is selected, the WPA authentication protocol of the second version for corporate Wi-Fi networks is used.

- **WPA2-Personal.**

If this item is selected, the WPA authentication protocol of the second version for personal Wi-Fi networks is used.

The **Any** item is selected by default.

Encryption type

Items in this drop-down list define the type of encryption used to protect Wi-Fi network traffic. Wi-Fi networks that use the specified type of encryption are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** Device Control mode.

The following items are available from the **Encryption type** drop-down list:

- **Any.**

If this item is selected, the type of encryption is not considered when determining whether or not a Wi-Fi network belongs to the trusted group.

- **Disconnected.**

If this item is selected, Wi-Fi networks that do not use encryption are considered trusted.

- **WEP.**

If this item is selected, Wi-Fi networks that use the Wired Equivalent Privacy algorithm are considered trusted. WEP is based on a stream cipher that allows using a variable key length.

- **TKIP.**

If this item is selected, the Wi-Fi networks that use the Temporal Key Integrity Protocol are considered trusted. A new key is generated for every packet that is transmitted. Keys are generated automatically and sent by the authentication server.

- **AES.**

If this item is selected, the Wi-Fi networks that use the Advanced Encryption Standard symmetrical block cipher algorithm with keys 128, 192, or 256 bits long are considered trusted. The level of encryption (128, 192, or 256 bits) determines the number of number of transformations applied to the data being encrypted.

The **Any** item is selected by default.

Comment. This entry field lets you specify any additional information about the rule according to which a Wi-Fi network is assigned to the trusted group.

Select trusted devices window

In this window, the administrator can add a device to trusted list.

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

The following actions are available for working with trusted devices:

- Add the device to the list of trusted devices.
- Change the user and / or user group that is allowed to access the trusted device.
- Delete the device from the list of trusted devices.

If you have added a device to the list of trusted devices and created an access rule for this type of device which blocks or restricts access, Kaspersky Endpoint Security decides whether or not to grant access to the device based on its presence in the list of trusted devices. Presence in the list of trusted devices has a higher priority than an access rule.

To add a device to the trusted list, the following settings are available:

Display connected devices

The items in this drop-down list determine the size of the list of connected devices:


- **Currently.** If this item is selected, the list of connected devices includes the devices that are currently connected to the computer.

This item is selected by default.

- **For the entire runtime.** If this item is selected, the list of connected devices displays devices that have been connected to the computer since installation of the current operating system.

Search field

In the search field, you can enter the full name or any number of characters from the name of the device that you want to add to the list of trusted devices. The table under the search field displays all devices whose names contain the characters that are entered in the search field.

To reset the search results, delete the contents of the search field or click the  button in the search field.

Connected devices

A table listing devices connected to the computer during the period of time selected in the **Display connected devices** drop-down list.

You can sort the list of connected devices by their names. To do so, click the header of the **Devices** column.

After you click the header of the **Devices** column, Kaspersky Endpoint Security sorts the list of connected devices in reverse alphabetical order. After you click the header of the **Devices** column for the second time, Kaspersky Endpoint Security sorts the list of connected devices in strict alphabetical order.

The table contains the following columns:

- **Devices.** This column shows the names of devices.

The check box next to the name of a device allows you to select the device and add it to the list of trusted devices:

- If the check box is selected, the device is selected to be added to the list of trusted devices.
- If the check box is cleared, the device is not selected to be added to the list of trusted devices.
- **State.** This column displays the state of device connections to the computer:
 - The *Connected* state means that the device is currently connected to the computer.
 - The *Disconnected* state means that the device is currently disconnected from the computer.

Comment

Additional information on the device.

Allow to users and / or groups of users

A field that lists users and / or groups of users. Those users and / or groups of users are granted full access (read and write) to the device that is selected from the table above.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window you can select the users and / or groups of users to which you want to grant access to devices.

Request access to device window

In this window, the user can generate a request access file for the blocked device and activate the access key received from the corporate LAN administrator.

The following settings are available:

Display connected devices

The items in this drop-down list determine the size of the list of connected devices:

- **Currently.** If this item is selected, the list of connected devices includes the devices that are currently connected to the computer.

This item is selected by default.

- **For the entire runtime.** If this item is selected, the list of connected devices displays devices that have been connected to the computer since Kaspersky Endpoint Security was installed.

Search field

In the search field, you can enter the full name or any number of characters from the name of the device to which you want to request access. The table under the search field displays all devices whose names contain the characters that are entered in the search field.

To clear search results, click the  button in the search field.

Devices

This column displays the names of devices.

You can sort the list of devices by their names. To do so, click the header of the **Devices** column.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of devices in reverse alphabetical order. After you click the header of the column for the second time, Kaspersky Endpoint Security sorts the list of devices in strict alphabetical order.

State

This column displays the state of device connections to the computer:

- The *Connected* state means that the device is currently connected to the computer.
- The *Disconnected* state means that the device is currently disconnected from the computer.

Generate request access file

Clicking this button opens the **Creating request access file** window. In this window, you can specify the required duration of access to a device and save the device request access file you have created.

Activate access key. Clicking this button opens the **Activating the access key for the device** window. This window lets you select a file with a device access key received from the LAN administrator.

Creating request access file window

In this window, the user can generate a request access file for the blocked device.

The following settings are available:

Access duration

This field allows you to specify the time interval (in hours) for which the user wants to receive access to the device.

Save

This button opens a standard window of Microsoft Windows named **Save access key** that lets you save the device access key file.

Anti-Virus protection

Kaspersky Endpoint Security provides comprehensive computer protection against various types of threats, network and phishing attacks.

Each type of threat is handled by a dedicated component. Components can be enabled or disabled independently of one another, and their settings can be configured.

In addition to the real-time protection that the application components provide, we recommend that you regularly *scan* the computer for viruses and other threats. This helps to rule out the possibility of spreading malware that is undetected by protection components due to a low security level setting or for other reasons.

Anti-virus protection components refer to the following application components:

- **File Anti-Virus.** This component protects the file system of the computer from infection. File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer and on all connected drives. File Anti-Virus intercepts every attempt to access a file and scans the file for viruses and other threats.
- **Mail Anti-Virus.** This component scans incoming and outgoing email messages for viruses and other threats.
- **Web Anti-Virus.** This component scans traffic that arrives on the user's computer via the HTTP and FTP protocols, and checks whether URLs are listed as malicious or phishing web addresses.
- **IM Anti-Virus.** This component scans traffic that arrives on the computer via IM client protocols. The component lets you securely use many IM clients.
- **System Watcher.** This component keeps a record of application activity on the computer and provides this information to other components to ensure more effective protection of the computer.

The following virus scan tasks are provided in Kaspersky Endpoint Security:

- **Full Scan.** Kaspersky Endpoint Security scans the operating system, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.
- **Custom Scan.** Kaspersky Endpoint Security scans the objects that are selected by the user.
- **Critical Areas Scan.** Kaspersky Endpoint Security scans objects that are loaded at operating system startup, RAM, and objects that are targeted by rootkits.

Anti-Virus protection section

Start Kaspersky Endpoint Security 10.0 for Windows at computer startup

The check box enables / disables the automatic start of Kaspersky Endpoint Security after the operating system loads.

When the check box is selected, Kaspersky Endpoint Security is started after the operating system loads, protecting the computer during the entire session.

When the check box is cleared, Kaspersky Endpoint Security is not started after the operating system loads until the user starts it manually. Computer protection is disabled and user data may be exposed to threats.

This check box is selected by default.

Use advanced disinfection technology

Advanced disinfection technology is available if Kaspersky Endpoint Security is installed on a computer that runs under Microsoft Windows for workstations. Advanced Disinfection technology is unavailable if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This check box enables / disables the function used by Kaspersky Endpoint Security to enable Advanced Disinfection technology for the computer.

When the check box is selected, on detecting malicious activity in the operating system Kaspersky Endpoint Security shows a pop-up message that suggests performing a special advanced disinfection procedure. After the user approves this procedure, Kaspersky Endpoint Security neutralizes and removes the threat from the computer. After completing the advanced disinfection

procedure, Kaspersky Endpoint Security restarts the computer. The advanced disinfection technology uses considerable computing resources, which may slow down other applications.

When the check box is cleared, upon detecting malicious activity in the operating system, Kaspersky Endpoint Security performs the disinfection procedure according to the current values of settings. No computer restart is performed after Kaspersky Endpoint Security neutralizes the threat.

This check box is cleared by default.

The **Objects** section lets you select the types of objects that Kaspersky Endpoint Security monitors while it is running.

Settings

Clicking this button opens the **Threats** window. In this window, you can modify the list of threats that Kaspersky Endpoint Security detects.

Regardless of the settings, Kaspersky Endpoint Security always detects viruses, worms, and Trojans.

The **Scan exclusions and trusted applications** section lets you create a list of objects which Kaspersky Endpoint Security does not monitor while it is running.

The list shows the number of the specified scan exclusions and trusted applications. The first number shows how many rules in the corresponding section are enabled. The second number shows the total number of rules configured in the corresponding section, including disabled rules.

Settings

This button opens the **Trusted zone** window. This window lets you create a list of exclusions, which may include a list of exclusion rules and a list of trusted applications.

A *trusted zone* is a list of objects and applications that Kaspersky Endpoint Security does not monitor when active. In other words, the trusted zone is a set of exclusions from the scope of Kaspersky Endpoint Security protection.

You create a trusted zone depending on the features of the objects that you handle and on the applications that are installed on the computer. You may need to compile a list of exclusion rules or

a list of trusted applications if, for example, Kaspersky Endpoint Security blocks access to an object or application which you know to be absolutely safe.

The **Monitored ports** section lets you select the network port monitoring mode in which Mail Anti-Virus, Web Anti-Virus, and File Anti-Virus scan incoming and outgoing data streams.

Monitor all network ports

In this network port monitoring mode, the protection components monitor data streams that are transmitted via any open network ports of the computer.

Monitor selected ports only

In this network port monitoring mode, the protection components monitor only user-specified ports.

A list of network ports that are normally used for transmission of email and network traffic is included in the application distribution kit.

This network port monitoring mode is selected by default.

Settings

This button opens the **Network ports** window. This window lets you create a list of monitored network ports and a list of applications for which Kaspersky Endpoint Security monitors all ports.

This button is available when the **Monitor only selected ports** network port monitoring mode is selected.

Objects for detection window

The **Malware** section lets you gain protection against objects that are categorized as Malicious programs.

Viruses, worms

This check box enables protection against viruses and worms.

Regardless of the application settings, Kaspersky Endpoint Security always detects and blocks viruses and worms. They can cause significant harm to the computer.

Protection against them cannot be disabled.

Trojans

This check box enables protection against Trojans.

Regardless of the application settings, Kaspersky Endpoint Security always detects and blocks Trojans. They can cause significant harm to the computer.

Protection against trojans cannot be disabled.

Malicious tools

This check box enables / disables protection against malicious tools.

When the check box is selected, protection against malicious tools is enabled.

This check box is selected by default.

The **Adware, auto-dialers, other programs** section lets you control adware and legal software that may be used by criminals to damage your computer or personal data.

Adware

This check box enables / disables protection against adware.

When the check box is selected, protection against adware is enabled.

This check box is selected by default.

Auto-dialers

This check box enables / disables protection against auto-dialers.

When the check box is selected, protection against auto-dialers is enabled.

This check box is selected by default.

Other

This check box enables / disables protection against legitimate applications that may be exploited by criminals to harm the user's computer or data (such as Internet chat clients, downloaders, monitoring programs, and remote administration applications).

If the check box is selected, protection is enabled.

This check box is cleared by default.

The **Compressed files** section enables protection against objects that are categorized as Packers.

Packed files that may cause harm

This check box enables / disables protection against packers that can be used by criminals to harm the computer or user data.

When the check box is selected, protection is enabled against packers that intruders can use to harm your computer or personal data.

This check box is selected by default.

Multi-packed files

This check box enables / disables protection against files which have been packed three or more times.

When the check box is selected, protection against multi-packed files is enabled.

This check box is selected by default.

Scan exclusions tab

In this window, the administrator can form a list of exclusions from Anti-Virus scan.

The following settings are available:

Scan exclusions

This table contains information about scan exclusions.

You can exclude the following objects from scanning:

- Files of certain formats
- Files that are selected by a mask
- Selected files
- Folders
- Objects according to the classification of Kaspersky Lab's Virus Encyclopedia

The table contains the following columns:

- **File or folder.** This column contains the check box and the path to a file or folder that has been excluded from scanning by Kaspersky Endpoint Security.

If the check box next to the name of an exclusion is selected, Kaspersky Endpoint Security applies this exclusion during the virus scan.

- **Object name.** This column shows the name of an object that has been excluded from scanning by Kaspersky Endpoint Security. Kaspersky Endpoint Security applies this exclusion if a scan for viruses and other threats detects an object with the specified name.
- **Comment.** This column shows information about a scan exclusion. For a scan exclusion that has been added by default, the column displays information about the vendor.

Add

Clicking this button opens the **Exclusion rule** window. You can create a new exclusion rule in this window.

Edit

Clicking this button opens the **Exclusion rule** window. You can edit the settings of the selected exclusion rule in this window.

This button is available when an element is selected in the **Exclusion rules** table.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete the selected exclusion rule from the list of exclusion rules.

This button is available if an item is selected in the exclusions table.

The **Scan exclusion description** section lets you view the description of the selected exclusion.

This section contains information when an item is selected in the **Scan exclusions** table.

Links in the **Scan exclusion description** section let you edit the settings of the selected exclusion.

File or folder

This item shows the full path to a file or folder that has been specified for the exclusion, in the form of a link. Clicking this link opens the **Name of file or folder** window. You can specify a different file or folder in this window.

This item is available if a file or folder has been selected for the exclusion.

Object name

This item shows the object name that has been specified for the exclusion, in the form of a link. Clicking the link opens the **Object name** window. In this window, you can change the full name of an object according to the classification of the Kaspersky Lab Virus Encyclopedia, or the object name by mask.

This item is available if an object name is selected for the exclusion.

Protection components: any / specified

This element lets you restrict an exclusion to one or more components.

If the **any** value is displayed in the form of a link, all Kaspersky Endpoint Security components apply this exclusion during scanning. Clicking this link causes its value to change to **specified**. The **select components** link appears.

If the **specified** value is displayed in the form of a link, the selected Kaspersky Endpoint Security components apply this exclusion during scanning. Clicking this link causes its value to change to **any**.

The list of components is available when components are selected for the exclusion. Clicking the **select components** link opens the **Protection components** window. This window lets you modify the contents of components that are associated with this exclusion.

Import

Clicking this button opens the standard **Open file** window in Microsoft Windows. In this window, you can select a file with the .dat extension to import a list of scan exclusions.

Export

Clicking this button opens the standard **Save as** window in Microsoft Windows. In this window, you can select a folder and specify the name of the .dat file that contains a list of scan exclusions.

Scan exclusion window

In this window, the administrator can specify the settings of an object added to the list of exclusions.

The following settings are available:

File or folder

This check box enables / disables an option that excludes the selected file or folder from the scan for viruses and other threats.

If the check box is selected, Kaspersky Endpoint Security creates an exclusion for the specified file or folder. Kaspersky Endpoint Security skips them during scanning.

The **File or folder** check box is selected by default in every exclusion.

Object name

This check box enables / disables the option that excludes an object from scanning by its name as it appears in the Kaspersky Lab Virus Encyclopedia.

If the check box is selected, Kaspersky Endpoint Security creates an exclusion for objects with the specified name and excludes objects with the specified name from the scan.

If the **File or folder** and **Object name** check boxes are both selected, Kaspersky Endpoint Security creates an exclusion for the specified file or folder which contains an object with the specified name. In this case, the following conditions apply:

- If a file and object name are specified, only the file containing the object with the specified name is excluded from all subsequent scans.
- If a folder and object name are specified, files in the specified folder which contain objects with the specified name are excluded from all subsequent scans.

Comment

A field for entering additional information about the exclusion rule.

The **Scan exclusion description** section contains a description of the exclusion. You can edit the exclusion settings and specify the Kaspersky Endpoint Security components that use this exclusion in their operation.

Links

Links can be used to edit the settings of an exclusion.

File or folder: select file or folder

Clicking this link opens the **Name of file or folder** window. In this window, you can specify the name of a file or folder to be skipped by Kaspersky Endpoint Security. You can also specify a file name mask.

This link is available when the **File or folder** check box is selected.

Object name: enter the object name

Clicking this link opens the **Object name** window. This window lets you specify an object name to have the application exclude objects with the specified name from the scan. The value is specified according to the classification of the Kaspersky Lab Virus Encyclopedia. You can also specify an object name by mask.

The link is available when the **Object name** check box is selected.

Protection components: any / specified

The **any** link signifies that this exclusion is used by all components of Kaspersky Endpoint Security.

The **specified** link signifies that this exclusion is used only by the selected components of Kaspersky Endpoint Security.

Clicking the **select components** link opens the **Protection components** window. This window lets you select the components that subsequently use this exclusion in their operation. The **select components** link is displayed if the **specified** link is displayed.

The **any** link is displayed by default.

Protection components window

In this window, the administrator can select which protection components will not perform a virus scan of the specified object.

The following settings are available:

Protection components

List of protection components and tasks of Kaspersky Endpoint Security that use the exclusion rule.

If the check box next to the name of a Kaspersky Endpoint Security protection component or task is selected, that component or task uses the exclusion rule.

By default, all check boxes are cleared for all Kaspersky Endpoint Security protection components and tasks.

Object name window

In this window, the administrator can specify the name of an object added to the list of exclusions.

The following settings are available:

Object name

A field for entering the object name or object name mask. The value is specified according to the classification of the Kaspersky Lab Virus Encyclopedia. Clicking the link www.securelist.com/en/descriptions takes you to the website of the Kaspersky Lab Virus Encyclopedia, which contains details of the object.

For example:

- **not-a-virus:RiskWare.RemoteAdmin.Win32.RAdmin21** – Remote Administrator application designed for remote control of computers; Version 2.1. Author — Dmitry Znosko, project page – www.famatech.com. In some configurations, the application can be exploited stealthily by an intruder.
- **HackTool.Win32.NetSend** is a hacker tool. It is a Windows program (PE EXE file). It was written in Microsoft Visual C++® and has a size of 10,752 bytes. It is packed by UPX. The unpacked file size is approximately 48 KB. This program serves for sending messages to

other computers on the Internet or LAN by using the built-in Windows Messenger Service. The program allows the sender's name to be spoofed. The startup settings involve transmitting the details of the target computer, the spoofed name of the sending computer, and the message text.

File or folder name window

In this window, the administrator can select a file or folder added to the list of exclusions from Anti-Virus scan.

The following settings are available:

File or folder name

A field for entering the file or folder name or mask of the file or folder name.

You can also specify the full path to a file or folder manually. Only file name masks with full paths to files can be entered.

For example:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** – All files in the C:\dir\ folder.
- **C:\dir*.exe** – All files with the .exe extension in the C:\dir\ folder.
- **C:\dir*.ex?** – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- **C:\dir\test** – Only the file C:\dir\test.

Browse

This button opens the **Select folder** window. This window lets you select an object in the object tree.

Include subfolders

This check box enables / disables an option whereby a folder is added to the exclusion rule with all subfolders.

When the check box is selected, Kaspersky Endpoint Security does not scan the folder with all of its subfolders.

When the check box is cleared, Kaspersky Endpoint Security does not scan only the specified folder.

This check box is selected by default.

Trusted applications tab

In this window, the administrator can generate a list of trusted applications whose activity will not be monitored by Kaspersky Endpoint Security.

The following settings are available:

Trusted applications

This table lists trusted applications whose activity is not monitored by Kaspersky Endpoint Security during its operation.

The table contains the following columns:

- **Application.** This column displays a check box and the name of a trusted application.

If the check box next to the name of a trusted application is selected, Kaspersky Endpoint Security scans this application in accordance with the list of exclusions.

The svchost.exe process is added by default.

- **Path.** This column shows the full path to the executable file of a trusted application.

Add

This button opens a context menu. The context menu contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window lists applications that are installed on the computer. You can select any application which you do not want Kaspersky Endpoint Security to scan.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. The Open window of Microsoft Windows lets you select the executable file of the application which you do not want Kaspersky Endpoint Security to scan.

Edit

Clicking the button opens the **Scan exclusions for application** window. Use this window to modify the list of application activity types that are skipped during scanning.

This button is available when an element is selected in the **Trusted applications** table.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete a trusted application from the list of trusted applications. Kaspersky Endpoint Security then scans this application during its operation.

This button is available when an element is selected in the **Trusted applications** table.

Import

Clicking this button opens the standard **Open file** window in Microsoft Windows. In this window, you can select a file with the .dat extension to import a list of trusted applications.

Export

Clicking this button opens the standard **Save as** window in Microsoft Windows. In this window, you can select a folder to save the .dat file that contains a list of trusted applications for export.

Exclusions for application window

In this window, the administrator can select which actions of an application added to the trusted list should not be monitored by Kaspersky Endpoint Security.

The following settings are available:

Do not scan opened files

This check box enables / disables the exclusion of all files opened by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan the files that the application opens.

Do not monitor application activity

This check box enables / disables the monitoring of file and network activity of an application in the operating system by the Application Privilege Control, System Watcher, and Firewall components.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of the application.

Do not inherit restrictions of the parent process (application)

This check box enables / disables inheritance by the application of application control rules and application network rules that are specified for the parent process (application).

If the check box is selected, Kaspersky Endpoint Security monitors application activity according to the rules that are specified by the system administrator: file activity is monitored according to application control rules, while network activity is monitored according to application network rules.

If the check box is cleared, Kaspersky Endpoint Security monitors application activity according to application control rules and the application network rules that are inherited from the parent process (application).

Do not monitor child application activity

This check box enables / disables the monitoring of file and network activity of any child application of this application.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of child applications of this application.

Do not block interaction with the application interface

The check box enables / disables permission for the application to interact with the Kaspersky Endpoint Security interface.

If the check box is selected, the remote access application is allowed to manage Kaspersky Endpoint Security settings through the Kaspersky Endpoint Security interface.

Do not scan network traffic

This check box enables / disables the exclusion of network traffic generated by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan incoming and outgoing traffic of this application according to the network traffic exclusion settings. You can configure the exclusion settings in the section that is below the **Do not scan network traffic** setting.

In the section below the **Do not scan network traffic** setting, you can edit the settings of network traffic exclusion from virus scanning.

The section is available if the **Do not scan network traffic** check box is selected.

any / specified remote IP addresses

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote IP addresses.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote IP addresses.

Clicking the **specify** link opens the **Remote IP addresses** window. This window lets you specify the list of IP addresses that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

any / specified remote ports

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote ports.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote ports.

Clicking the **specify** link opens the **Remote ports** window. This window lets you specify the list of remote ports that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

Trusted system certificate store tab

In this window, the administrator can select a trusted system certificate store to be used by Kaspersky Endpoint Security to generate a list of exclusions from Anti-Virus scan.

The following settings are available:

Use trusted system certificate store

This check box enables / disables the use of the trusted system certificate storage.

If the check box is selected, Kaspersky Endpoint Security excludes from scanning the applications signed with a trusted digital signature. The Application Privilege Control component automatically assigns such applications to the Trusted group.

If the check box is cleared, a virus scan is performed regardless of whether or not the application has a digital signature. The Application Privilege Control component assigns applications to trust groups according to the configured settings.

This check box is cleared by default.

Trusted system certificate store

Items in this drop-down list define which system certificate storage is considered trusted by Kaspersky Endpoint Security.

The default setting is **Enterprise Trust**.

Network ports window

In this window, the administrator can specify the monitored network ports. Kaspersky Endpoint Security will scan the network activity of applications passing through these ports. The administrator can also select individual applications whose network traffic will be scanned when passing through the monitored ports.

The following settings are available:

Network ports

This table contains network ports and protocols that are normally used for transmission of email and network traffic. This list is included in the Kaspersky Endpoint Security package.

If the check box in this row is selected, Kaspersky Endpoint Security monitors network traffic that passes through this network port via any network protocol.

If the check box in this row is cleared, Kaspersky Endpoint Security temporarily excludes the network port from scanning, but does not remove it from the list of network ports.

By default, all check boxes are selected.

The table contains the following columns:

- **Description.** This column shows the name of the network protocol under which network traffic is transferred through the port most often. The number of the port is indicated in the **Port** column.
- **Port.** This column shows the number of the network port.

Add

Clicking this link opens the **Network port** window. This window lets you add a new network port to the list of network ports that are monitored by Kaspersky Endpoint Security.

Edit

Clicking this link opens the **Network port** window. This window lets you change the network port that is monitored by Kaspersky Endpoint Security.

This link is available when an item is selected in the **Network ports** list.

Delete

Clicking this link causes Kaspersky Endpoint Security to delete the selected network port from the list of network ports.

This link is available when an item is selected in the **Network ports** list.

Monitor all ports for specified applications

This check box enables / disables the option whereby all network ports are monitored for applications that are specified in the **Applications** list.

When the check box is selected, Kaspersky Endpoint Security monitors all network ports for applications that request network access. You can specify these applications in the **Applications** list.

This check box is selected by default.

Applications

A table of applications for which Kaspersky Endpoint Security monitors all network ports. For each application, the path to its executable file is specified. The default list of applications for which Kaspersky Endpoint Security monitors all network ports has been created by Kaspersky Lab.

If the check box next to an application is selected, Kaspersky Endpoint Security monitors all network ports of the application.

If the check box next to an application is cleared, Kaspersky Endpoint Security temporarily does not monitor all network ports of the application.

The check boxes are selected for all applications by default.

The table is available if the **Monitor all ports for specified applications** check box is selected.

The table contains the following columns:

- **Application.** This column shows the application name.
- **Path.** This column shows the path to the executable file of the application.

Add

If you use the local interface of Kaspersky Endpoint Security to generate a list of applications whose network activity should be monitored by Firewall via the above-mentioned ports, clicking the **Add** link opens the context menu. The context menu contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window lists applications that are installed on the computer. From the list of applications, you can select any application for which you want Kaspersky Endpoint Security to monitor all network ports.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. This window lets you specify the executable file of an application for which you want Kaspersky Endpoint Security to monitor all network ports.

If you use the Kaspersky Endpoint Security 10.0 for Windows administration plug-in to generate a list of applications whose network activity should be monitored by Firewall via the network ports specified above, clicking the **Add** link opens the **Application** window. In this window, you can specify the path to the executable file and the application name.

Edit

Clicking this link opens the **Application** window. This window lets you edit the settings of an application for which Kaspersky Endpoint Security monitors all network ports.

This link is available if an item is selected from the **Applications** list.

Delete

This link deletes the selected application from the list of applications.

This link is available if an item is selected from the **Applications** list.

The **Information** section contains warnings about changes that are made to the list of network ports and to the list of applications.

Network port window

In this window, the administrator can add a port to the list of ports monitored by the application.

The following settings are available:

Port

A field for entering the number of the monitored network port.

For example, port 1080.

Description

A field for entering the name of the monitored network port.

Application window

In this window, the administrator can add an application to the list of applications whose network activity is scanned when passing through the monitored ports.

The following settings are available:

Path

A field for entering the path to the executable file of an application for which Kaspersky Endpoint Security monitors all network ports.

Name

A field for entering the name of an application for which Kaspersky Endpoint Security monitors all network ports.

Protecting the computer file system. File Anti-Virus

This section contains information about File Anti-Virus and instructions on how to configure the component settings.

In this section:

About File Anti-Virus	155
File Anti-Virus subsection	155

About File Anti-Virus

File Anti-Virus prevents infection of the computer's file system. By default, File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer and on all drives that are attached to it for the presence of viruses and other threats.

On detecting a threat in a file, Kaspersky Endpoint Security performs the following:

1. Detects the type of object detected in the file (such as a *virus* or *trojan*).
2. Labels the file as *probably infected* if the scan cannot determine whether or not the file is infected. The file may contain a code sequence that is typical of viruses or other malware, or the modified code of a known virus.
3. The application displays a notification about the malicious object detected in the file (if notifications are configured), and processes the file by taking the action specified in the File Anti-Virus settings.

File Anti-Virus subsection

Enable File Anti-Virus

This check box enables / disables File Anti-Virus.

If the check box is selected, File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer. By default, File Anti-Virus is configured with the settings that are recommended by Kaspersky Lab specialists.

If the check box is cleared, File Anti-Virus is disabled.

This check box is selected by default.

In the **Security level** section, you can select one of the three file security levels that have been created by Kaspersky Lab specialists, or configure file security level settings on your own. When deciding on a file security level, be sure to take working conditions and the current situation into account.

High

When this file security level is selected, File Anti-Virus takes the strictest control of all files that are opened, saved, and started. File Anti-Virus scans all file types on all hard drives, network drives, and removable storage media of the computer. It also scans archives, installation packages, and embedded OLE objects.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists. File Anti-Virus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer. It also scans embedded OLE objects. File Anti-Virus does not scan archives or installation packages.

The **Recommended** file security level is the default setting.

Low

The settings of this file security level ensure maximum scanning speed. File Anti-Virus scans only files with specified extensions on all hard drives, network drives, and removable storage media of the computer. File Anti-Virus does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

This button opens the **File Anti-Virus** window. In this window, you can configure file security level settings.

By default

This button sets the file security level to **Recommended**.

The **Action on threat detection** section allows you to select the action that File Anti-Virus performs if infected files are detected during scanning.

Before attempting to disinfect or delete an infected file, File Anti-Virus creates a backup copy for subsequent restoration or disinfection.

Select action automatically

If this option is selected, Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. This action is **Select action: Disinfect. Delete if disinfection fails**.

This action is selected by default.

Perform action: Disinfect. Delete if disinfection fails

If this option is selected, File Anti-Virus automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, File Anti-Virus deletes those files.

To select the **Perform action: Disinfect. Delete if disinfection fails** action, select the **Perform action** setting and select the **Disinfect** and **Delete if disinfection fails** check boxes.

Perform action: Disinfect

If this option is selected, File Anti-Virus automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, File Anti-Virus moves those files to Quarantine.

To select the **Perform action: Disinfect** action, select the **Perform action** setting, select the **Disinfect** check box, and clear the **Delete if disinfection fails** check box.

Perform action: Delete

If this option is selected, File Anti-Virus automatically deletes all infected or probably infected files that it detects.

To select the **Perform action: Delete** action, select the **Perform action** setting, clear the **Disinfect** check box, and select the **Delete** check box.

Perform action: Block

If this option is selected, File Anti-Virus automatically blocks all infected or probably infected files without attempting to disinfect them.

To select the **Perform action: Block** action, select the **Perform action** setting and clear the **Delete if disinfection fails** and **Disinfect** check boxes.

General tab

The **File types** section allows you to select the types of files that File Anti-Virus scans.

File Anti-Virus treats files without extensions as executables. File Anti-Virus always scans them, regardless of the file types that are selected for scanning.

All files

If this setting is selected, File Anti-Virus scans all files without exceptions (all formats and extensions).

Files scanned by format

If this setting is selected, File Anti-Virus scans only potentially infectable files. Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file (for example, .txt, .doc, or .exe). During scanning, the extension of the file is also taken into account.

This is the default setting.

Files scanned by extension

If this setting is selected, File Anti-Virus scans only potentially infectable files. The file format is then determined based on the file's extension.

Icon ⓘ.

Clicking the icon opens the Help system section of Kaspersky Endpoint Security. This section describes a list of file extensions that are scanned by File Anti-Virus.

The **Protection scope** section allows you to create the list of objects that are scanned by File Anti-Virus.

Protection scope

Contains objects that are scanned by File Anti-Virus. A scan object may be a hard drive or network drive, folder, file, or file name mask.

By default, File Anti-Virus scans files that are started on any hard drives, network drives, or removable drives. Objects that are in the **Protection scope** list by default cannot be edited or removed.

If the check box next to the name of a scan object is selected, File Anti-Virus scans it.

If the check box next to the name of a scan object is cleared, File Anti-Virus temporarily excludes it from scanning.

Add

Clicking this button opens the **Select scan scope** window. In this window, you can select objects to be scanned.

Edit

Clicking this button opens the **Select scan scope** window. In this window, you can edit the path to an object to scan.

This button is available if a non-default object has been selected from the list of objects to scan.

Delete

This button removes the selected scan object from the **Protection scope** list.

This button is available if a non-default object has been selected from the list of objects to scan.

Select scan scope window

In this window, the administrator can select an object to add to the scan scope of File Anti-Virus.

The following settings are available:

Object

This field displays the path to the object that is selected from the folder tree above. You can specify a hard drive or network drive, folder, file, or file name mask as an object to be scanned.

You can also enter the path to a scan object manually.

File name masks must be entered with full paths to objects. For example:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** – All files in the C:\dir\ folder.
- **C:\dir*.exe** – All files with the .exe extension in the C:\dir\ folder.
- **C:\dir*.ex?** – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- **C:\dir\test** – Only the file C:\dir\test.
-

Add

This button adds the path to the selected scan object or file name mask to the **Protection scope** list on the **General** tab of the **File Anti-Virus** window.

Include subfolders

This check box enables / disables scanning of folders that are inside the selected folder. If a subfolder contains other child folders, they are scanned as well. Kaspersky Endpoint Security scans subfolders of all levels.

This check box is selected by default.

List of files scanned by extension

If you selected **Files scanned by extension** in the **File types** section, File Anti-Virus or the virus scan task thoroughly analyzes files with certain extensions for the presence of viruses and other malware.

Kaspersky Endpoint Security considers files without an extension as executable ones.
Kaspersky Endpoint Security always scans executable files regardless of the file types that you select for scanning.

The actual format of a file may not match its file name extension.

File Anti-Virus or the virus scan task scans files with the following extensions:

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

Ink – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

eml – Microsoft Outlook Express message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – extension for a saved Microsoft Office Outlook message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file. Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows.

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates,.xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsx for Microsoft Office Excel 2007 templates with macro support, and xlsm for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

Performance tab

The **Scan methods** section contains methods that File Anti-Virus uses when scanning the computer.

Signature Analysis

Signature analysis uses the Kaspersky Endpoint Security database that contains descriptions of known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security.

Following the recommendations of Kaspersky Lab's experts, this method is always enabled.

Heuristic Analysis

This check box enables / disables Heuristic Analysis during scanning of the computer.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of detail of Heuristic Analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium scan** and **Deep scan** levels. Scanning is faster and less resource-intensive.

The **Light scan** detail level is set by default.

- **Medium scan.** While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
- **Deep scan.** While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

Scan only new and changed files

This check box enables / disables the mode of scanning only new files and files that have been modified since the previous scan. File Anti-Virus scans both plain and compound files.

If the mode of scanning only new and modified files is enabled, the links for selecting scanning of all or only new files in the **Scan of compound files** section (**all / new**) become unavailable.

This check box is selected by default.

The **Scan of compound files** section contains a list of compound files that File Anti-Virus scans for viruses and malware.

Scan archives

This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

This check box is cleared by default.

The following scan options are available for archives:

- **All.** File Anti-Virus scans all archives.
- **New.** File Anti-Virus scans only new archives that have appeared after the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables / disables scanning of installation packages.

This check box is cleared by default.

The following scan options are available:

- **All.** File Anti-Virus scans all installation packages.
- **New.** File Anti-Virus scans only new installation packages that have appeared since the last scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan Office formats

This check box enables / disables the feature that File Anti-Virus uses during a virus scan to scan Office format files, including embedded OLE objects.

This check box is selected by default.

The following scan options are available:

- **All.** File Anti-Virus scans all Office format files.
- **New.** File Anti-Virus scans only new Office format files that have appeared since the time of the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Additional

This button opens the **Compound files** window. In this window, you can specify settings for scanning of compound files.

Compound files window

The **Background scan** section allows you to reduce the time that is required to scan large compound files.

Extract compound files in the background

This check box enables / disables the option of reducing the delay when opening large compound files.

If the check box is selected, Kaspersky Endpoint Security unpacks compound files whose size exceeds the value that is specified in the **Minimum file size** field in the background and with a delay after their detection. Such files can be available for use while they are being scanned. Compound files with a size that is less than the value that is specified in the **Minimum file size** field are available for use only after they are unpacked and scanned.

If the check box is cleared, Kaspersky Endpoint Security unpacks all compound files. Compound files are available for use only after they are unpacked and their contents are scanned.

This check box is cleared by default.

Kaspersky Endpoint Security always scans files that are extracted from archives.

Minimum file size

Field for entering the minimum size of compound files that are available for use while being scanned by Kaspersky Endpoint Security. The value is specified in megabytes.

By default, the file size is set to 0 MB.

The **Size limit** section allows you to limit scanning of compound files that are of a specified size.

Do not unpack large compound files

If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the value that is specified in the **Maximum file size** field.

If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

Maximum file size

Kaspersky Endpoint Security does not unpack files that are larger than the specified value. The value is specified in megabytes.

By default, the file size is set to 8 MB.

Additional tab

The **Scan mode** section allows you to select a condition that triggers file scanning by File Anti-Virus.

Smart mode

In this scan mode, File Anti-Virus scans files by analyzing operations that are performed with a file by the user, an application on behalf of the user (under the currently active account or a different user account), or the operating system.

This mode is used by default.

On access and modification

In this scan mode, File Anti-Virus scans files when the user or an application on behalf of the user (under the currently active account or a different user account) or the operating system attempts to open or modify the files.

On access

In this scan mode, File Anti-Virus scans files only when the user or an application on behalf of the user (under the currently active account or a different user account) or the operating system attempts to open the files.

On execution

In this scan mode, File Anti-Virus scans files only when the user or an application on behalf of the user (under the currently active account or a different user account) or the operating system attempts to launch the files.

The **Scan technologies** section contains scan technologies that File Anti-Virus uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. This speeds up anti-virus scanning of objects that are from various file systems and operating systems.

iSwift Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any changes made to the scan settings. The iSwift technology is an improvement on the iChecker technology for the NTFS file system.

The check box enables / disables the use of iSwift technology.

This check box is selected by default.

iChecker Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.

The check box enables / disables the use of iChecker technology.

This check box is selected by default.

The **Pause task** section allows you to pause File Anti-Virus.

By schedule

The check box enables / disables the option that allows pausing File Anti-Virus for a specified time. This feature can decrease the load on the operating system.

This check box is cleared by default.

Schedule

This button opens the **Pause task** window. In this window, you can specify the time interval for which File Anti-Virus is paused.

The button is available if the **By schedule** check box is selected.

At application startup

This check box enables / disables the option which pauses File Anti-Virus for the time period during which the user works with applications that require significant resources from the operating system.

This check box is cleared by default.

Select

This button opens the **Applications** window. In this window, you can create a list of applications that pause File Anti-Virus when they are running.

The button is available if the **At application startup** check box is cleared.

Pause task window

In this window, the administrator can specify the time to pause and resume File Anti-Virus.

The following settings are available:

Pause task at

Field for entering the time at which File Anti-Virus pauses. The time is specified in HH:MM format.

Resume task at

Field for entering the time at which File Anti-Virus resumes. The time is specified in HH:MM format.

Applications window

In this window, the administrator can form a list of applications that, when started, will cause File Anti-Virus to terminate its operation.

The following settings are available:

Applications

This list includes applications during whose operation Kaspersky Endpoint Security pauses File Anti-Virus. For each application the list includes the path to its corresponding executable file.

Add

This button opens a context menu. The context menu contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window displays a list of applications that are currently running. You can select any application from the list.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. In this window, you can specify the executable application file that you are adding to the list.

Edit

This button opens a context menu. Use context menu items to replace the application that is selected from the list with another one. The context menu of the button contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window displays a list of applications that are currently running. You can select any application from the list.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. In this window, you can specify the executable application file that you want to use to replace the one from the list in the **Applications** window.

This button is available if an item is selected from the **Applications** list.

Delete

This button removes the selected application from the list.

This button is available if an item is selected from the **Applications** list.

Select application window

In this window, the administrator can add an application that, when started, will cause File Anti-Virus to terminate its operation.

The following settings are available:

Search field

In the search field, you can enter the full name of an application or a keyword from its name to find the application in the **Select application from the list** table. All applications with names that

contain the characters that are entered in the search field are displayed in the table under the search field.

To reset the search results, delete the contents of the search field.

Select application from the list

This table displays the applications that are installed on the user's computer.

The table contains the following columns:

- **Application.** This column shows the name of an application that is installed on the user's computer.
- **Vendor.** This column displays the name of the vendor of an application that is installed on the user's computer.
- **File.** This column shows the full path to the executable file of the application.

Email protection. Mail Anti-Virus

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Mail Anti-Virus and instructions on how to configure the component settings.

In this section:

About Mail Anti-Virus.....	173
Mail Anti-Virus subsection	174

About Mail Anti-Virus

Mail Anti-Virus scans incoming and outgoing email messages for viruses and other threats. It starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all messages that are sent or received via the POP3, SMTP, IMAP, MAPI, and NNTP protocols. If no threats are detected in the message, it becomes available and/or is processed.


On detecting a threat in an email message, Mail Anti-Virus performs the following:

1. Identifies the type of object detected in the email message (such as a *trojan*).
2. An email message is assigned one of the following statuses:
 - *Probably infected*. This status is assigned if the scan cannot determine whether or not the email message is definitely infected. The email message may possibly contain a section of code that is typical of viruses or other malware, or the modified code of a known virus.

- *Infected.* This status is assigned to an object if the scan of an email message finds a section of code of a known virus that is included in the anti-virus databases of Kaspersky Endpoint Security.
- *Not found.* This status is assigned to an object if the scan of an email message does not detect viruses or other threats.

The application then blocks the email message, displays a notification about the detected object (if this is specified in the notification settings), and performs the action that is specified in the settings of Mail Anti-Virus.

This component interacts with mail clients installed on the computer. An embeddable extension is available for the Microsoft Office Outlook® mail client that lets you fine-tune the message scan settings. The Mail Anti-Virus extension is embedded in the Microsoft Office Outlook mail client during installation of Kaspersky Endpoint Security.

Operation of Mail Anti-Virus is signified by the application icon displayed in the taskbar notification area. When Mail Anti-Virus is scanning an email message, the application icon changes to .

Mail Anti-Virus subsection

Enable Mail Anti-Virus

This check box enables / disables Mail Anti-Virus.

When the check box is selected, Mail Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all email messages that are transmitted via the POP3, SMTP, IMAP, MAPI, and NNTP protocols.

When the check box is cleared, Mail Anti-Virus is disabled.

This check box is selected by default.

The **Security level** section allows you to select one of three email security levels that are preconfigured by Kaspersky Lab's experts, or configure a custom email security level on your own. When deciding on an email security level, be sure to take into account the working conditions and current situation.

High

When this email security level is selected, Mail Anti-Virus performs the strictest control of email messages. Mail Anti-Virus scans incoming and outgoing messages, and performs deep heuristic analysis.

The **High** mail security level is recommended when working in a dangerous environment. An example of such an environment is a connection to a free email service from a home network that is not guarded by centralized email protection.

Recommended

The email security level that provides the optimal balance between the performance of Kaspersky Endpoint Security and email security. Mail Anti-Virus scans incoming and outgoing email messages, and performs medium-level heuristic analysis. This mail traffic security level is recommended by Kaspersky Lab specialists.

The **Recommended** mail security level is the default setting.

Low

When this email security level is selected, Mail Anti-Virus only scans incoming email messages, performs light heuristic analysis, and does not scan archives that are attached to email messages. At this mail security level, Mail Anti-Virus scans email messages at maximum speed and uses a minimum of operating system resources.

The **Low** mail security level is recommended for use in a well-protected environment. An example of such an environment might be a LAN with centralized email security.

Custom

Email security level with your custom settings.

Settings

This button opens the **Mail Anti-Virus** window. In this window, you can configure the email security level settings.

By default

This button sets the email security level to **Recommended**.

The **Action on threat detection** section allows you to select the action that Mail Anti-Virus performs if scanning reveals that an email message is infected.

Before attempting to disinfect or delete an infected email message, Mail Anti-Virus creates a backup copy of it for subsequent restoration or disinfection.

Select action automatically

If this option is selected, Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. This action is **Select action: Disinfect. Delete if disinfection fails**.

This action is selected by default.

Perform action: Disinfect. Delete if disinfection fails

If this option is selected, Mail Anti-Virus automatically attempts to disinfect all infected or probably infected email messages that are detected. If disinfection fails, Mail Anti-Virus deletes them.

To select the **Perform action: Disinfect. Delete if disinfection fails** action, select the **Perform action** setting and select the **Disinfect** and **Delete if disinfection fails** check boxes.

Perform action: Disinfect

If this option is selected, Mail Anti-Virus automatically attempts to disinfect all infected or probably infected email messages that are detected. If disinfection fails, Mail Anti-Virus moves them to Quarantine.

To select the **Perform action: Disinfect** action, select the **Perform action** setting, select the **Disinfect** check box, and clear the **Delete if disinfection fails** check box.

Perform action: Delete

If this option is selected, Mail Anti-Virus automatically deletes all infected or probably infected email messages that are detected.

To select the **Perform action: Delete** action, select the **Perform action** setting, clear the **Disinfect** check box, and select the **Delete** check box.

Perform action: Block

If this option is selected, Mail Anti-Virus automatically blocks all infected or probably infected email messages without attempting to disinfect them.

To select the **Perform action: Block** action, select the **Perform action** setting and clear the **Delete if disinfection fails** and **Disinfect** check boxes.

General tab

The **Protection scope** section allows you to select the type of email messages that are scanned by Mail Anti-Virus.

Incoming and outgoing messages

If this setting is selected, Mail Anti-Virus scans both incoming and outgoing email messages.

This is the default setting.

Incoming messages only

If this option is selected, Mail Anti-Virus scans only incoming email messages.

The **Connectivity** section lets you configure the scanning of email traffic by Mail Anti-Virus and the settings of Mail Anti-Virus embedding into email clients.

POP3 / SMTP / NNTP / IMAP traffic

The check box enables / disables scanning by Mail Anti-Virus of traffic that is transferred via the POP3, SMTP, NNTP, and IMAP protocols before it arrives on the receiving computer.

If the check box is selected, Mail Anti-Virus scans email messages that arrive via the POP3, SMTP, NNTP, and IMAP protocols before they are received on the computer.

When the check box is cleared, Mail Anti-Virus does not scan email messages that are transferred via the POP3, SMTP, NNTP, and IMAP protocols before they arrive on your computer. In this case, email messages are scanned by the Mail Anti-Virus plug-in that is embedded in Microsoft Office Outlook email client after email messages arrive on the user's computer.

This check box is selected by default.

Additional: Microsoft Office Outlook extension

If the check box is selected, you can configure the Mail Anti-Virus settings from Microsoft Office Outlook and specify when Mail Anti-Virus should scan email messages for viruses. Scanning of email messages transmitted via POP3, SMTP, NNTP, IMAP, and MAPI protocols is enabled on the

side of the extension integrated into Microsoft Office Outlook. Scanning is performed after messages have been received on the user's computer.

If the check box is cleared, Mail Anti-Virus settings cannot be configured from Microsoft Office Outlook. Scanning of email messages transmitted via POP3, SMTP, NNTP, IMAP, and MAPI protocols after they have been received on the user's computer is disabled on the side of the extension integrated into Microsoft Office Outlook.

This check box is selected by default.

The **Scan of compound files** section contains the settings for scanning objects attached to email messages.

Scan attached archives

This check box enables / disables the option where Mail Anti-Virus scans archives that are attached to email messages.

This check box is selected by default.

Scan attached Office formats

This check box enables / disables the option where Mail Anti-Virus scans Office format files that are attached to email messages.

This check box is selected by default.

Do not scan archives larger than

The check box enables / disables the option where Mail Anti-Virus scans archives that are attached to email messages depending on the size of the archives. This feature can accelerate scanning of email messages.

The maximum size of archives attached to email messages is specified in megabytes.

By default, the value is set to 8 MB.

If this check box is selected, Mail Anti-Virus excludes archives attached to email messages from scanning if their size exceeds the specified value. A field for specifying the maximum size of archives attached to email messages.

If the check box is cleared, Mail Anti-Virus scans email attachment archives of any size.

This check box is cleared by default.

The check box is available if the **Scan attached archives** check box is selected.

Do not scan archives for more than

The check box enables / disables the option that limits the amount of time that is allocated for scanning archives attached to email messages.

The maximum scan time for archives attached to email messages is specified in seconds.

The default value is 5 seconds.

If the check box is selected, the time that is allocated for scanning archives attached to email messages is limited to the specified period. A field for specifying the maximum time for scanning archives attached to email messages.

This check box is cleared by default.

The check box is available if the **Scan attached archives** check box is selected.

Email protection window

In this window, the administrator can configure the email scan settings using the Mail Anti-Virus extension for Outlook.

The following settings are available:

Scan when receiving

This check box enables / disables the scanning of email messages as they are received.

If the check box is selected, Mail Anti-Virus analyzes each message as it arrives to the mailbox.

If the check box is cleared, Mail Anti-Virus does not scan a message as it is received.

This check box is selected by default.

Scan when reading

This check box enables / disables the scanning of email messages when they are read.

If the check box is selected, Mail Anti-Virus scans a message when the user opens it to read it.

If the check box is cleared, Mail Anti-Virus does not scan a message when it is opened to be read.

This check box is selected by default.

Scan when sending

This check box enables / disables the scanning of email messages as they are sent.

If the check box is selected, Mail Anti-Virus analyzes each outgoing message as it is being sent.

If the check box is cleared, Mail Anti-Virus does not scan outgoing messages as they are being sent.

This check box is selected by default.

If mail is scanned using the Mail Anti-Virus extension for Outlook, it is recommended to use Cached Exchange Mode. For more detailed information about the Exchange caching mode and recommendations on its use, please refer to the Microsoft Knowledge Base:

<https://technet.microsoft.com/en-us/library/cc179175.aspx>.

Attachment filter tab

In this window, the administrator can configure a filter by which Mail Anti-Virus will pick out email message attachments to undergo a virus scan.

The following settings are available:

Disable filtering

If this setting is selected, Mail Anti-Virus does not filter files that are attached to email messages.

This is the default setting.

Rename selected attachment types

If this setting is selected, Mail Anti-Virus replaces the last character in attached files of the specified types with the underscore (_) symbol.

Delete selected attachment types

If this setting is selected, Mail Anti-Virus deletes attached files of the specified types from email messages.

You can specify the types of attached files to delete from email messages in the list of file masks.

File masks

A list of file masks that Mail Anti-Virus either renames or deletes after filtering attachments in email messages.

The list of file masks is available if the **Rename specified attachment types** option or the **Delete specified attachment types** option is enabled.

If the check box next to the file mask is selected, Mail Anti-Virus renames or deletes files of this type when filtering email attachments.

If the check box next to the file mask is cleared, Mail Anti-Virus skips files of this type without any changes when filtering email attachments.

Add

This button opens the **File mask** window. In this window, you can enter a file mask to add to the list of file masks.

Edit

This button opens the **File mask** window. In this window, you can change an existing file mask.

The button is available if an item in the list of file masks is selected.

Delete

This button deletes the selected item from the list of file masks.

The button is available if an item in the list of file masks is selected.

File mask window

In this window, the administrator can specify a mask for files forwarded in email attachments that must be scanned by Mail Anti-Virus.

The following setting is available:

File mask

The field for entering the file mask in accordance with which Mail Anti-Virus filters attachments in email messages.

Additional tab

In this window, the administrator can configure the heuristic analysis settings for Mail Anti-Virus.

The following settings are available:

Heuristic Analysis

This check box enables / disables the use of heuristic analysis during Mail Anti-Virus email scans.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the heuristic analysis level. The heuristic analysis level ensures a balance between the thoroughness of scanning for threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of heuristic analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning email for malicious code. At this heuristic analysis level, the probability of detecting threats is lower than at the **medium scan** and **deep scan** heuristic analysis levels. Email scanning is faster and less resource-intensive.
- **Medium scan.** When scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.

The **medium scan** heuristic analysis level is selected by default.

- **Deep scan.** When scanning mail for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **light scan** and **medium scan** levels of heuristic analysis. At this heuristic analysis level, the probability of detecting threats is higher than at

the **Light** and **Medium** levels of heuristic analysis. Email scanning consumes more system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

Computer protection on the Internet. Web Anti-Virus

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Web Anti-Virus and instructions on how to configure the component settings.

In this section:

About Web Anti-Virus	184
Web Anti-Virus subsection	185

About Web Anti-Virus

Every time you go online, you expose information that is stored on your computer to viruses and other malware. They can infiltrate the computer while the user is downloading free software or browsing websites that are compromised by criminals. Network worms can find a way onto your computer as soon as you establish an Internet connection, even before you open a web page or download a file.

Web Anti-Virus protects incoming and outgoing data that is sent to and from the computer over the HTTP and FTP protocols and checks URLs against the list of malicious or phishing web addresses.

Web Anti-Virus intercepts and analyzes for viruses and other threats every web page or file that is accessed by the user or an application via the HTTP or FTP protocol. The following happens next:

- If the page or file is found not to contain malicious code, the user gains immediate access to them.

- If a user accesses a web page or file that contains malicious code, the application performs the action that is specified in the Web Anti-Virus settings.

Web Anti-Virus subsection

Enable Web Anti-Virus

This check box enables / disables Web Anti-Virus.

If the check box is selected, Web Anti-Virus protects information that arrives on the computer via the HTTP and FTP protocols.

If the check box is cleared, Web Anti-Virus is disabled.

This check box is selected by default.

The **Security level** section allows you to select one of three security levels for web traffic that are preconfigured by Kaspersky Lab, or configure your own custom security level. When deciding on the web traffic security level, be sure to take into account the working conditions and current situation.

High

The security level under which Web Anti-Virus performs maximum scanning of web traffic that the computer receives via the HTTP and FTP protocols. Web Anti-Virus thoroughly scans all web traffic objects using the full set of application databases, and performs the deepest possible heuristic analysis.

Recommended

The security level that provides the optimal balance between the performance of Kaspersky Endpoint Security and the security of web traffic. Web Anti-Virus performs heuristic analysis at the **medium scan** level. This web traffic security level is recommended by Kaspersky Lab specialists.

The **Recommended** web traffic security level is set by default.

Low

The settings of this web traffic security level ensure the fastest scanning of web traffic. Web Anti-Virus performs heuristic analysis at the **light scan** level.

Custom

Web traffic security level with your custom settings.

Settings

This button opens the **Web Anti-Virus** window. In this window you can configure the security level settings for web traffic.

By default

This button sets the web traffic security level to **Recommended**.

The **Action on threat detection** section allows you to select an action to be performed by Web Anti-Virus if scanning web traffic reveals that an object contains malicious code.

Select action automatically

If this action is selected, on detection of an infected object in web traffic Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. The default action is **Block download**.

Block download

If this action is selected, on detection of an infected object Web Anti-Virus blocks access to the object and displays a notification about the action.

This action is selected by default.

Allow download

If this action is selected, on detection of an infected object Web Anti-Virus allows the object to be downloaded to your computer.

General tab

In this window, the administrator can select the scan methods used by Web Anti-Virus, and configure the anti-phishing settings.

The following settings are available:

Check if web addresses are listed in the database of malicious web addresses

This check box enables / disables the option to scan web addresses against the database of malicious web addresses.

Checking web addresses against the database of malicious web addresses helps to detect websites that are in the black list of web addresses. The database of malicious web addresses is maintained by Kaspersky Lab, included in the application installation package, and updated during Kaspersky Endpoint Security database updates.

This check box is selected by default.

Heuristic analysis for detecting viruses

The check box enables / disables the use of heuristic analysis when scanning web traffic for viruses and other malware.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the heuristic analysis level of web traffic for viruses and other malicious programs. The heuristic analysis level ensures a balance between the thoroughness of scanning for threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of heuristic analysis of web traffic for viruses and other malicious programs are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files when scanning web traffic for malicious code. At this heuristic analysis level, the probability of detecting threats is lower than at the **medium scan** and **deep scan** heuristic analysis levels. Web traffic scanning is faster and less resource-intensive.
- **Medium scan.** When scanning web traffic for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab. This heuristic analysis level is selected by default.
- **Deep scan.** When scanning web traffic for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **light scan** and **medium scan** levels of heuristic analysis. At this heuristic analysis level, the probability of detecting threats is higher than at the **Light** and **Medium** levels of heuristic analysis. Web traffic scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis for detecting viruses** check box is selected.

Check if web addresses are listed in the database of phishing web addresses

This check box enables / disables the option to scan links to determine if they are in the database of phishing web addresses.

The database of phishing web addresses includes the web addresses of currently known websites that are used to launch phishing attacks. Kaspersky Lab supplements this database with web addresses that are obtained from the Anti-Phishing Working Group, an international organization. The database of phishing addresses is included in the application installation package and supplemented with Kaspersky Endpoint Security database updates.

The check box is selected by default.

Heuristic analysis for detecting phishing links

The check box enables / disables the use of heuristic analysis when scanning web pages for phishing links.

This check box is selected by default.

Trusted URLs tab

In this window, the administrator can form a list of trusted addresses from which web traffic will not be scanned.

The following settings are available:

Do not scan web traffic from trusted URLs

The check box enables / disables scanning of the content of web pages / websites whose addresses are included in the list of trusted web addresses.

If the check box is selected, Web Anti-Virus does not scan the content of web pages / websites whose addresses are included in the list of trusted web addresses.

If the check box is cleared, Web Anti-Virus scans the content of all opened web pages / websites.

This check box is selected by default.

Trusted web addresses

Contains the web addresses of web pages / websites whose content you trust. Web Anti-Virus does not scan the content of web pages / websites whose addresses are included in the list of trusted web addresses. You can add both the address and the address mask of a web page / website to the list of trusted addresses.

If the check box next to the web address of the web page / website is selected, Web Anti-Virus scans the content of the web page / website.

If the check box next to the URL of the web page / website is cleared, Web Anti-Virus temporarily excludes it from the list of trusted URLs and does not check its contents.

Add

This button opens the **Address / Address mask** window. In this window you can enter the address or address mask of the web page / website to be added to the list of trusted web addresses.

Edit

This button opens the **Address / Address mask** window. In this window, you can change the address or address mask of the web page / website that is added to the list of trusted web addresses.

The button is available if the address or address mask of the web page or website is selected.

Delete

This button removes the selected address or address mask of the web page / website from the list of trusted web addresses.

The button is available if the address or address mask of the web page or website is selected.

Web address / Web address mask window

In this window, the administrator can specify a web address or web address mask to be added to the trusted list.

The following settings are available:

Web address / Web address mask

Input field for the address or address mask of the web page / website.

For example, the address www.virus.com.

The following characters can be used to generate the address mask of the web page / website:

- * replaces any sequence of characters.

For example, Web Anti-Virus interprets the address mask `*abc*` as any web address that contains the sequence `abc` (for example, `www.virus.com/download_virus/page_0-9abcdef.html`).

- ? – Any single character.

For example, Web Anti-Virus interprets the address mask `Patch_123?.com` as any URL that contains the sequence `Patch_123?.com` and any character after the character 3 (for example, `patch_12345.com`).

If the URL contains the characters `*` and `?`, the `\` character needs to precede each of them. This is a special screening character, which indicates that the following character is to be interpreted not as a special symbol, but as any ordinary one. If the URL address includes the `\` character, it too must be preceded by the `\` character.

For example, `www.virus.com/download_virus/virus.dll\?virus_name=`.

Protection of IM client traffic. IM Anti-Virus

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about IM Anti-Virus and instructions on how to configure the component settings.

In this section:

About IM Anti-Virus	191
IM Anti-Virus subsection.....	192

About IM Anti-Virus

IM Anti-Virus scans the traffic of instant messaging clients (known as *IM clients*).

IM Anti-Virus does not scan messages transmitted over encrypted channels.

Messages that are sent through IM clients can contain the following kinds of security threats:

- URLs that attempt to download a malicious program to the computer
- URLs to malicious programs and websites that intruders use for phishing attacks

The goal of phishing attacks is to steal the personal data of users, such as bank card numbers, passport details, passwords for bank payment systems and other online services (such as social networking sites or email accounts).

Files can be transmitted through IM clients. When you attempt to save such files, they are scanned by the File Anti-Virus component (see section "About File Anti-Virus" on page [155](#)).

IM Anti-Virus intercepts every message that the user sends or receives through an IM client and scans it for links that may threaten the security of the computer:

- If no dangerous URLs are detected in the message, it becomes available to the user.
- If dangerous links are detected in the message, IM Anti-Virus replaces the message with information about the threat in the message window of the active IM client.

IM Anti-Virus subsection

Enable IM Anti-Virus

This check box enables / disables IM Anti-Virus.

If the check box is selected, IM Anti-Virus starts together with Kaspersky Endpoint Security, remains constantly in the computer's RAM, and scans all messages that arrive through IM clients. IM Anti-Virus lets you use many instant messengers safely, including ICQ, MSN® Messenger, AIM®, Mail.Ru Agent and IRC.

If the check box is cleared, IM Anti-Virus is disabled.

This check box is selected by default.

The **Protection scope** section lets you select the type of messages that are transmitted by IM clients to be scanned by IM Anti-Virus.

Incoming and outgoing messages

If this setting is enabled, IM Anti-Virus scans both incoming and outgoing messages of IM clients for malicious objects or links that are in databases of suspicious and / or phishing web addresses.

This is the default setting.

Incoming messages only

If this setting is enabled, IM Anti-Virus scans only incoming messages of IM clients for malicious objects or web addresses that are in databases of malicious and phishing web addresses. IM Anti-Virus does not scan outgoing messages.

The **Scan methods** section contains methods that IM Anti-Virus uses when scanning messages that arrive through IM clients.

Check if web addresses are listed in the database of malicious web addresses

This check box enables / disables the scanning of web addresses in IM client messages against the database of malicious web addresses.

The database of malicious web addresses is maintained by Kaspersky Lab and is included in the application distribution kit.

This check box is selected by default.

Check if web addresses are listed in the database of phishing web addresses

This check box enables / disables scanning of web addresses in IM client messages against the database of phishing web addresses.

The Kaspersky Endpoint Security database of phishing web addresses includes websites that are known to be used in phishing attacks. Kaspersky Lab supplements this database with web addresses that are obtained from the Anti-Phishing Working Group, an international organization. The database of phishing web addresses is updated during Kaspersky Endpoint Security database updates.

This check box is selected by default.

System Watcher

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about System Watcher and instructions on how to configure the component settings.

In this section:

About System Watcher.....	194
System Watcher subsection.....	195

About System Watcher

System Watcher collects data on the actions of applications on your computer and passes this information to other components for more reliable protection.

Behavior stream signatures

Behavior Stream Signatures (BSS) (also called "behavior stream signatures") contain sequences of application actions that Kaspersky Endpoint Security classifies as dangerous. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the specified action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

By default, if application activity fully matches a behavior stream signature, System Watcher moves the executable file of that application to Quarantine.

Rolling back actions that have been performed by malware

Based on information collected by System Watcher, Kaspersky Endpoint Security can roll back actions that have been performed by malware in the operating system while performing disinfection.

A rollback of malware actions can be initiated by File Anti-Virus (see page [155](#)) or during a virus scan (see section "Scanning the computer" on page [199](#)).

Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data.

System Watcher subsection

In this window, the administrator can perform the following operations:

- Enable or disable System Watcher.
- enable or disable exploit protection;
- Configure the System Watcher settings for applications on client computers.
- Configure the settings for using behavior stream signatures (BSS).
- Enable or disable rollback of actions performed by malware in the system.

The following settings are available:

Enable System Watcher

This check box enables / disables the operation of the System Watcher component.

If the check box is selected, the functionality that is specified in the System Watcher settings is enabled.

If the check box is cleared, the functionality that is specified in the System Watcher settings is disabled.

This check box is selected by default.

Enable Exploit Prevention

This check box enables / disables the Exploit Prevention feature.

If the check box is selected, Kaspersky Endpoint Security keeps track of executable files launched by vulnerable applications. On detecting that an attempt to run an executable file from a vulnerable application was not initiated by the user, Kaspersky Endpoint Security blocks the launch of this file. Information about the blocked launch of the executable file is stored in the Exploit Prevention report.

This check box is selected by default.

Do not monitor the activity of digitally signed applications

The check box enables / disables the function that adds digitally signed applications to the Trusted group.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

If the check box is selected, Kaspersky Endpoint Security adds digitally signed applications to the Trusted group. Kaspersky Endpoint Security does not monitor the activities of applications from this group.

If the check box is cleared, Kaspersky Endpoint Security does not add digitally signed applications to the Trusted group.

This check box is selected by default.

On detecting malware activity

The items in this drop-down list determine the action that Kaspersky Endpoint Security performs on detection of malicious activity:

- **Select action automatically.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. By default, Kaspersky Endpoint Security moves the executable file of the malicious application to Quarantine.

This action is selected by default.

- **Move file to Quarantine.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security moves the executable file of this application to Quarantine.
- **Terminate the malicious program.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security terminates this application.
- **Skip.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security does not take any action on the executable file of the application.

Roll back malware actions during disinfection

This check box enables / disables the function of Kaspersky Endpoint Security that allows rolling back malware actions in the operating system while disinfection is in progress.

If the check box is selected, Kaspersky Endpoint Security rolls back malware actions in the operating system while disinfection is in progress.

This check box is selected by default.

Scanning the computer

A virus scan is vital to computer security. Regularly run virus scans to rule out the possibility of spreading malware that is undetected by protection components due to a low security level setting or for other reasons.

This section describes the specifics and settings of scan tasks, security levels, scan methods and technologies, and instructions on handling files which Kaspersky Endpoint Security has not processed during a virus scan.

In this section:

About scan tasks.....	199
Scheduled tasks section.....	200

About scan tasks

To find viruses and other types of malware and check the integrity of application modules, Kaspersky Endpoint Security includes the following tasks:

- **Full Scan.** A thorough scan of the entire computer. By default, Kaspersky Endpoint Security scans the following objects:
 - Kernel memory
 - Objects that are loaded at startup of the operating system
 - Boot sectors
 - Operating system backup
 - All hard and removable drives
- **Critical Areas Scan.** By default, Kaspersky Endpoint Security scans the kernel memory, running processes, and disk boot sectors.

- **Custom Scan.** Kaspersky Endpoint Security scans the objects that are selected by the user. You can scan any object from the following list:
 - Kernel memory
 - Objects that are loaded at startup of the operating system
 - Operating system backup
 - Outlook mailbox
 - All hard, removable, and network drives
 - Any selected file
- **Integrity Check.** Kaspersky Endpoint Security checks the application modules for corruption or modifications.

The Full Scan and Critical Areas Scan tasks are somewhat different than the others. For these tasks, it is not recommended to edit the scan scope.

After scan tasks start, their completion progress is displayed in the field next to the name of the running scan task in the **Tasks** section on the **Protection and Control** tab of the main window of Kaspersky Endpoint Security.

Information on the scan results and events that have occurred during the performance of scan tasks is logged in a Kaspersky Endpoint Security report.

Scheduled tasks section

The **Task run mode** section lets you configure the settings of the run mode of scheduled tasks.

Settings

This button opens the **Run mode** tab with the name of a task. On the **Run mode** tab, you can configure the run mode of the scheduled task.

The **Background scan** section lets you configure a virus scan to pause during activity by the user on the client computer with Kaspersky Endpoint Security installed.

Perform Idle Scan

This check box enables / disables an option that starts a scan task for autorun objects, the kernel memory, and the operating system partition when the computer is locked or the screensaver is on for 5 minutes or longer, if one of the following conditions is true:

- An idle scan of the computer has not been performed since installation of Kaspersky Endpoint Security.
- The previous idle scan of the computer was completed more than 7 days ago.
- The previous idle scan of the computer was interrupted during an update of the application databases and modules.
- The previous idle scan of the computer was interrupted during an on-demand scan.

If the check box is selected, the idle scan task starts when one of the preceding conditions is true.

If the check box is cleared, the idle scan task does not start.

This check box is cleared by default.

The **Scan removable drives on connection** section lets you select the action that Kaspersky Endpoint Security performs when you connect a removable drive to the computer.

Action on removable drive connection

This drop-down list lets you select the action that Kaspersky Endpoint Security performs when a removable drive is connected to the computer.

The drop-down list contains the following items:

- **Do not scan**

If this item is selected, Kaspersky Endpoint Security does not scan the removable drive.

This item is selected by default.

- **Detailed Scan**

If this item is selected, after a removable drive is connected Kaspersky Endpoint Security scans all files located on the removable drive, including files within compound objects.

- **Quick Scan**

If this item is selected, when a removable drive is connected Kaspersky Endpoint Security scans only files with specific extensions that are most vulnerable to infection, and does not unpack compound objects.

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

eml – Microsoft Outlook Express message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – extension for saved Microsoft Office Outlook emails

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file. Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows.

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates,.xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsx for Microsoft Office Excel 2007 templates with macro support, and xlsm for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

Maximum removable drive size

This check box enables / disables a limit on the size of removable drives on connection of which Kaspersky Endpoint Security performs the action that is selected in the **Actions on removable drive connection** drop-down list.

If this check box is selected, Kaspersky Endpoint Security performs the action that is selected in the **Actions on removable drive connection** drop-down list on removable drives with a size not more than the specified maximum drive size.

If the check box is cleared, Kaspersky Endpoint Security performs the action that is selected in the **Actions on removable drive connection** drop-down list on removable drives of any size.

Removable drive size is specified in megabytes. The default value is 4096 MB.

This setting is available if the **Full Scan** or **Quick Scan** action is selected in the **Actions on removable drive connection** drop-down list.

This check box is cleared by default.

Full Scan subsection

In the **Security level** section, you can select one of the three file security levels that have been created by Kaspersky Lab specialists, or configure file security level settings on your own. When deciding on a file security level, be sure to take working conditions and the current situation into account.

High

If the probability of computer infection is very high, select this file security level.

Kaspersky Endpoint Security scans all types of files. When scanning compound files, Kaspersky Endpoint Security also scans mail-format files.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists.

Kaspersky Endpoint Security scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Kaspersky Endpoint Security does not scan archives or installation packages.

The **Recommended** file security level is selected by default.

Low

The settings of this file security level ensure maximum scanning speed.

Kaspersky Endpoint Security scans only new or modified files with the specified extensions on all hard drives, removable drives, and network drives of the computer. Kaspersky Endpoint Security does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

This button opens the Full Scan task settings window.

By default

This button sets the file security level to **Recommended**.

The **Action on threat detection** section lets you select the action that Kaspersky Endpoint Security performs if the Full Scan task detects infected files.

Select action automatically

If this option is selected, Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. This action is **Select action: Disinfect. Delete if disinfection fails**.

Perform action: Disinfect. Delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

To select the **Perform action: Disinfect. Delete if disinfection fails** action, select the **Perform action** setting and select the **Disinfect** and **Delete if disinfection fails** check boxes.

This action is selected by default.

Perform action: Disinfect

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, the application moves them to Quarantine. Kaspersky Endpoint Security applies the **Delete** action to files that are part of the Windows Store application.

To select the **Perform action: Disinfect** action, select the **Perform action** setting, select the **Disinfect** check box, and clear the **Delete if disinfection fails** check box.

Perform action: Delete

If this option is selected, Kaspersky Endpoint Security automatically deletes all infected or probably infected files that are detected.

To select the **Perform action: Delete** action, select the **Perform action** setting, clear the **Disinfect** check box, and select the **Delete** check box.

Perform action: Inform

If this option is selected, on detecting infected or probably infected files Kaspersky Endpoint Security informs you of this and moves the detected files to Quarantine.

To select the **Perform action: Inform** action, select the **Perform action** setting and clear the **Delete if disinfection fails** and **Disinfect** check boxes.

The **Run mode and scan scope** section contains the settings that Kaspersky Endpoint Security uses to start the full computer scan task. You can also use this section to create lists of objects to be scanned by Kaspersky Endpoint Security when running the Full Scan task.

Run mode

Clicking this button opens the **Run mode** tab in the **Full Scan** window. This window lets you select the Full Scan task run mode.

To the right of the button, the current run mode of the Full Scan task is displayed.

Scan scope

Clicking this button opens the **Objects to scan** window. This window lets you specify the objects to be scanned by Kaspersky Endpoint Security during the Full Scan task.

Scope tab

The **File types** section lets you select the file types that Kaspersky Endpoint Security scans when performing the Full Scan task.

Kaspersky Endpoint Security considers files without an extension as executable ones.
Kaspersky Endpoint Security always scans executable files regardless of the file types that you select for scanning.

All files

If this setting is enabled, Kaspersky Endpoint Security checks all files without exception (all formats and extensions).

This is the default setting.

Files scanned by format

If this setting is selected, Kaspersky Endpoint Security scans only potentially infectable files. Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file (for example, .txt, .doc, or .exe). During scanning, the extension of the file is also taken into account.

Files scanned by extension

If this setting is selected, Kaspersky Endpoint Security scans only potentially infectable files. The file format is then determined based on the file's extension.

Icon ⓘ.

Clicking the icon opens the Help system section of Kaspersky Endpoint Security. This section lists file extensions that are scanned by Kaspersky Endpoint Security.

The **Scan optimization** section contains settings that you can use to reduce the time that is needed to perform the Full Scan task.

Scan only new and changed files

This check box enables / disables the mode of scanning only new files and files that have been modified since the previous scan. Kaspersky Endpoint Security scans both plain and compound files.

If the mode of scanning only new and modified files is enabled, the links for selecting scanning of all or of only new files in the **Scan of compound files** section (**all / new**) become unavailable.

Skip files scanned longer than

The check box enables / disables the time duration for scanning an object. After the specified amount of time, Kaspersky Endpoint Security stops scanning a file.

File scanning is stopped by default after 30 seconds.

The **Scan of compound files** section contains a list of compound files that Kaspersky Endpoint Security scans for viruses and other threats.

Scan archives

This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

This check box is cleared by default.

The following scan options are available for archives:

- **All.** File Anti-Virus scans all archives.
- **New.** File Anti-Virus scans only new archives that have appeared after the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables / disables scanning of installation packages.

This check box is cleared by default.

The following scan options are available:

- **All.** File Anti-Virus scans all installation packages.
- **New.** File Anti-Virus scans only new installation packages that have appeared since the last scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan Office formats

This check box enables / disables the feature that File Anti-Virus uses during a virus scan to scan Office format files, including embedded OLE objects.

This check box is selected by default.

The following scan options are available:

- **All.** File Anti-Virus scans all Office format files.
- **New.** File Anti-Virus scans only new Office format files that have appeared since the time of the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Parse email formats

Scan password-protected archives

If the check box is selected, Kaspersky Endpoint Security scans password-protected archives. Before files in an archive can be scanned, you are prompted to enter the password.

If the check box is cleared, Kaspersky Endpoint Security skips scanning of password-protected archives.

This check box is cleared by default.

Additional

This button opens the **Compound files** window. In this window, you can specify settings for scanning of compound files.

Compound files window

The **Size limit** section allows you to limit scanning of compound files that are of a specified size.

Do not unpack large compound files

If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the value that is specified in the **Maximum file size** field.

If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

Maximum file size

Kaspersky Endpoint Security does not unpack files, and only those files, that are larger than the specified value. The value is specified in megabytes.

Additional tab

The **Scan methods** section contains methods that Kaspersky Endpoint Security uses when scanning the computer.

Signature Analysis

Signature analysis uses the Kaspersky Endpoint Security database that contains descriptions of known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security.

Following the recommendations of Kaspersky Lab's experts, this method is always enabled.

Heuristic Analysis

This check box enables / disables Heuristic Analysis during scanning of the computer.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of detail of Heuristic Analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium scan** and **Deep scan** levels. Scanning is faster and less resource-intensive.

The **Light scan** detail level is set by default.

- **Medium scan.** While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
- **Deep scan.** While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

The **Scan technologies** section contains scan technologies that Kaspersky Endpoint Security uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. This speeds up anti-virus scanning of objects that are from various file systems and operating systems.

iSwift Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any changes made to the scan settings. The iSwift technology is an improvement on the iChecker technology for the NTFS file system.

The check box enables / disables the use of iSwift technology.

This check box is selected by default.

iChecker Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.

The check box enables / disables the use of iChecker technology.

This check box is selected by default.

Run mode tab

The **Run mode** section allows you to select the scan task run mode.

Manually

This scan task run mode allows you to start the scan task manually.

By schedule

In this scan task run mode, Kaspersky Endpoint Security starts the scan task in accordance with the schedule that you create. If this scan task run mode is selected, you can also start the scan task manually.

Frequency

The items in this drop-down list determine the start time of the scan task.

This setting is available if the **By schedule** scan task run mode is selected.

The following items are available from the **Frequency** drop-down list:

- **Minutes.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in minutes.

The **Run every N minutes** setting is available for this value. It specifies the interval between startups of the scan task, in minutes. The value cannot exceed 59 minutes. The default value is 5 minutes.

- **Hours.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in hours.

The **Run every N hours** setting is available for this item. It sets the interval between startups of the scan task, in hours. The value cannot exceed 23 hours. The default value is one hour.

- **Days.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in days.

The following settings are available for this item:

- **Run every.** The item specifies the interval between startups of the scan task, in days. The default value is one day.

The value cannot exceed 31 days.

- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **Every week.** If this item is selected, Kaspersky Endpoint Security starts the scan task on the specified days of the week.

The following settings are available for this item:

- **Start on.** The check boxes enable / disable startup of the scan task on the selected days of the week.
- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **At a specified time.** If you select this item, Kaspersky Endpoint Security starts the scan task on the specified day and at the specified time.

The **Start date and time** setting is available for this item. It specifies the day and time at which Kaspersky Endpoint Security starts the scan task. The date is specified in

DD / MM / YY format; the time is specified in HH:MM:SS format. By default, the current date is selected and the time is set to 0:00:00.

- **Every month.** If this item is selected, Kaspersky Endpoint Security starts the scan task once per month on the specified day and at the specified time.

The following settings are available for this item:

- **Run every N-th day of the month.** This setting specifies the day of the month on which Kaspersky Endpoint Security starts the scan task. The first day of the month is the default value.
- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **After application startup.** If this item is selected, Kaspersky Endpoint Security starts the scan task every time that Kaspersky Endpoint Security is started.

The **Start in** setting is available for this item. It specifies the interval (in minutes) since the startup of Kaspersky Endpoint Security after which Kaspersky Endpoint Security starts the scan task. The default value is 15 minutes.

- **After every update.** If this item is selected, Kaspersky Endpoint Security starts the scan task after each update.

Postpone running after application startup for

This setting specifies the time interval after the startup of Kaspersky Endpoint Security by which the start of the scan task is postponed.

Because a large number of processes start at operating system startup, it is convenient to start the scan task with a time delay after startup of Kaspersky Endpoint Security.

The default value is 15 minutes.

This setting is unavailable if the **After application startup** or **After every update** items are selected from the **Frequency** drop-down list.

Run skipped tasks

This check box enables / disables automatic startup of skipped scan tasks. For example, a scan task can be skipped if the computer was turned off when the scan task was set to start. If the check

box is selected, Kaspersky Endpoint Security starts the skipped scan task as soon as it becomes possible.

If the check box is cleared, Kaspersky Endpoint Security does not run skipped scan tasks. Instead, it carries out the next scan task in accordance with the current schedule.

This setting is unavailable if the **Minutes**, **Hours**, **After application startup**, or **After every update** items are selected from the **Frequency** drop-down list.

This check box is cleared by default.

Run only when the computer is idle

This check box enables / disables a function that suspends the start of the scan task when computer resources are limited. Kaspersky Endpoint Security starts the scan task when the screensaver is on and the computer is locked.

This check box is cleared by default.

The **User** section contains settings for starting the scan task under an account that differs from the one under which you have logged in to the operating system.

Run task as

This check box enables / disables the use of an account, which differs from the one under which you have logged in to the operating system, for starting the scan task.

If the check box is selected, Kaspersky Endpoint Security starts the scan task with the rights of the user that is specified in the **Name** field. The option is available for starting the scan task of Kaspersky Endpoint Security both manually and by a schedule.

If the check box is cleared, Kaspersky Endpoint Security starts the scan task under the current account that you have used to log in to the operating system.

This check box is cleared by default.

Name

A field for entering the name of the account under which the scan task is to be started.

This setting is available if the **Run task as** check box is selected.

Password

Field for entering the password for the account that is entered in the **Name** field.

This setting is available if the **Run task as** check box is selected.

Scan scope window

In this window, the administrator can form the scope of the virus scan.

The following settings are available:

Add

Clicking this button opens the **Select scan scope** window. In this window, you can add objects to be scanned.

Edit

Clicking this button opens the **Select scan scope** window. In this window, you can edit the path to an object to scan.

This button is available if a non-default object has been selected from the list of objects to scan.

Delete

This button deletes the selected scan object from the list of objects to scan.

This button is available if a non-default object has been selected from the list of objects to scan.

Scan scope. A list of objects to be scanned by Kaspersky Endpoint Security when running a scan task. Objects within the scan scope can include the kernel memory, running processes, boot sectors, system backup, mail databases, hard drives, removable drives or network drives, a folder or file.

If the check box next to the name of an object within the scan scope is selected, Kaspersky Endpoint Security scans this object.

If an object within the scan scope is cleared, Kaspersky Endpoint Security temporarily excludes this object from the scan.

By default, check boxes are selected next to all objects that have been added, except the **My email** and **All network drives** objects.

Select scan scope window

In this window, the administrator can select an object to be added to the virus scan scope.

The following settings are available:

Object

This field displays the path to the scan object that is selected from the folder tree above. You can specify a hard drive or network drive, folder, file, or file name mask as an object to be scanned.

You can also enter the path to a scan object manually.

File name masks must be entered with full paths to objects. For example:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** – All files in the C:\dir\ folder.
- **C:\dir*.exe** – All files with the .exe extension in the C:\dir\ folder.
- **C:\dir*.ex?** – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- **C:\dir\test** – Only the file C:\dir\test.

Add

This button adds the path to the selected object to be scanned or the file name mask to the list of objects to be scanned in the **Scan scope** window.

Include subfolders

This check box enables / disables scanning of folders that are inside the selected folder. If a subfolder contains other child folders, they are scanned as well. Kaspersky Endpoint Security scans subfolders of all levels.

This check box is selected by default.

Critical Areas Scan subsection

In the **Security level** section, you can select one of the three file security levels that have been created by Kaspersky Lab specialists, or configure file security level settings on your own. When

deciding on a file security level, be sure to take working conditions and the current situation into account.

High

If the probability of computer infection is very high, select this file security level.

Kaspersky Endpoint Security scans all types of files. When scanning compound files, Kaspersky Endpoint Security also scans mail-format files.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists.

Kaspersky Endpoint Security scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Kaspersky Endpoint Security does not scan archives or installation packages.

The **Recommended** file security level is selected by default.

Low

The settings of this file security level ensure maximum scanning speed.

Kaspersky Endpoint Security scans only new or modified files with the specified extensions on all hard drives, removable drives, and network drives of the computer. Kaspersky Endpoint Security does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

This button opens the Critical Areas Scan task settings window.

By default

This button sets the file security level to **High**.

The **Action on threat detection** section lets you select the action that is performed by Kaspersky Endpoint Security after the Critical Areas Scan detects infected files.

Select action automatically

If this option is selected, Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. This action is **Select action: Disinfect. Delete if disinfection fails.**

Perform action: Disinfect. Delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

To select the **Perform action: Disinfect. Delete if disinfection fails** action, select the **Perform action** setting and select the **Disinfect** and **Delete if disinfection fails** check boxes.

This action is selected by default.

Perform action: Disinfect

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, the application moves them to Quarantine. Kaspersky Endpoint Security applies the **Delete** action to files that are part of the Windows Store application.

To select the **Perform action: Disinfect** action, select the **Perform action** setting, select the **Disinfect** check box, and clear the **Delete if disinfection fails** check box.

Perform action: Delete

If this option is selected, Kaspersky Endpoint Security automatically deletes all infected or probably infected files that are detected.

To select the **Perform action: Delete** action, select the **Perform action** setting, clear the **Disinfect** check box, and select the **Delete** check box.

Perform action: Inform

If this option is selected, on detecting infected or probably infected files Kaspersky Endpoint Security informs you of this and moves the detected files to Quarantine.

To select the **Perform action: Inform** action, select the **Perform action** setting and clear the **Delete if disinfection fails** and **Disinfect** check boxes.

The **Run mode and scan scope** section contains settings that are used by Kaspersky Endpoint Security when starting the Critical Areas Scan task. You can also use this section to create lists of objects to be scanned by Kaspersky Endpoint Security when running the Critical Areas Scan task.

Run mode

Clicking this button opens the **Run mode** tab in the **Critical Areas Scan** window. This window lets you select the run mode of the Critical Areas scan task.

On the right of the button, the current task run mode is displayed.

Scan scope

Clicking this button opens the **Objects to scan** window. This window lets you specify the objects to be scanned by Kaspersky Endpoint Security during the Critical Areas Scan task.

Scope tab

The **File types** section lets you select the file types that Kaspersky Endpoint Security scans when performing the Critical Areas Scan task.

Kaspersky Endpoint Security considers files without an extension as executable ones.
Kaspersky Endpoint Security always scans executable files regardless of the file types that you select for scanning.

All files

If this setting is enabled, Kaspersky Endpoint Security checks all files without exception (all formats and extensions).

This is the default setting.

Files scanned by format

If this setting is selected, Kaspersky Endpoint Security scans only potentially infectable files. Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file (for example, .txt, .doc, or .exe). During scanning, the extension of the file is also taken into account.

Files scanned by extension

If this setting is selected, Kaspersky Endpoint Security scans only potentially infectable files. The file format is then determined based on the file's extension.

Icon .

Clicking the icon opens the Help system section of Kaspersky Endpoint Security. This section lists file extensions that are scanned by Kaspersky Endpoint Security.

The **Scan optimization** section contains settings that you can use to reduce the time that is needed to perform the Critical Areas Scan task.

Scan only new and changed files

This check box enables / disables the mode of scanning only new files and files that have been modified since the previous scan. Kaspersky Endpoint Security scans both plain and compound files.

If the mode of scanning only new and modified files is enabled, the links for selecting scanning of all or of only new files in the **Scan of compound files** section (**all / new**) become unavailable.

Skip files scanned longer than

The check box enables / disables the time duration for scanning an object. After the specified amount of time, Kaspersky Endpoint Security stops scanning a file.

File scanning is stopped by default after 30 seconds.

The **Scan of compound files** section contains a list of compound files that Kaspersky Endpoint Security scans for viruses and other threats.

Scan archives

This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

This check box is cleared by default.

The following scan options are available for archives:

- **All.** File Anti-Virus scans all archives.

- **New.** File Anti-Virus scans only new archives that have appeared after the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables / disables scanning of installation packages.

This check box is cleared by default.

The following scan options are available:

- **All.** File Anti-Virus scans all installation packages.
- **New.** File Anti-Virus scans only new installation packages that have appeared since the last scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan Office formats

This check box enables / disables the feature that File Anti-Virus uses during a virus scan to scan Office format files, including embedded OLE objects.

This check box is selected by default.

The following scan options are available:

- **All.** File Anti-Virus scans all Office format files.
- **New.** File Anti-Virus scans only new Office format files that have appeared since the time of the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Parse email formats

Scan password-protected archives

If the check box is selected, Kaspersky Endpoint Security scans password-protected archives. Before files in an archive can be scanned, you are prompted to enter the password.

If the check box is cleared, Kaspersky Endpoint Security skips scanning of password-protected archives.

This check box is cleared by default.

Additional

This button opens the **Compound files** window. In this window, you can specify settings for scanning of compound files.

Compound files window

The **Size limit** section allows you to limit scanning of compound files that are of a specified size.

Do not unpack large compound files

If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the value that is specified in the **Maximum file size** field.

If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

Maximum file size

Kaspersky Endpoint Security does not unpack files, and only those files, that are larger than the specified value. The value is specified in megabytes.

Additional tab

The **Scan methods** section contains methods that Kaspersky Endpoint Security uses when scanning the computer.

Signature Analysis

Signature analysis uses the Kaspersky Endpoint Security database that contains descriptions of known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security.

Following the recommendations of Kaspersky Lab's experts, this method is always enabled.

Heuristic Analysis

This check box enables / disables Heuristic Analysis during scanning of the computer.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of detail of Heuristic Analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium scan** and **Deep scan** levels. Scanning is faster and less resource-intensive.

The **Light scan** detail level is set by default.

- **Medium scan.** While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
- **Deep scan.** While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

The **Scan technologies** section contains scan technologies that Kaspersky Endpoint Security uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. This speeds up anti-virus scanning of objects that are from various file systems and operating systems.

iSwift Technology

iChecker Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.

The check box enables / disables the use of iChecker technology.

This check box is selected by default.

Run mode tab

The **Run mode** section allows you to select the scan task run mode.

Manually

This scan task run mode allows you to start the scan task manually.

By schedule

In this scan task run mode, Kaspersky Endpoint Security starts the scan task in accordance with the schedule that you create. If this scan task run mode is selected, you can also start the scan task manually.

Frequency

The items in this drop-down list determine the start time of the scan task.

This setting is available if the **By schedule** scan task run mode is selected.

The following items are available from the **Frequency** drop-down list:

- **Minutes.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in minutes.

The **Run every N minutes** setting is available for this value. It specifies the interval between startups of the scan task, in minutes. The value cannot exceed 59 minutes. The default value is 5 minutes.

- **Hours.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in hours.

The **Run every N hours** setting is available for this item. It sets the interval between startups of the scan task, in hours. The value cannot exceed 23 hours. The default value is one hour.

- **Days.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in days.

The following settings are available for this item:

- **Run every.** The item specifies the interval between startups of the scan task, in days. The default value is one day.

The value cannot exceed 31 days.

- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **Every week.** If this item is selected, Kaspersky Endpoint Security starts the scan task on the specified days of the week.

The following settings are available for this item:

- **Start on.** The check boxes enable / disable startup of the scan task on the selected days of the week.
- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **At a specified time.** If you select this item, Kaspersky Endpoint Security starts the scan task on the specified day and at the specified time.

The **Start date and time** setting is available for this item. It specifies the day and time at which Kaspersky Endpoint Security starts the scan task. The date is specified in DD / MM / YY format; the time is specified in HH:MM:SS format. By default, the current date is selected and the time is set to 0:00:00.

- **Every month.** If this item is selected, Kaspersky Endpoint Security starts the scan task once per month on the specified day and at the specified time.

The following settings are available for this item:

- **Run every N-th day of the month.** This setting specifies the day of the month on which Kaspersky Endpoint Security starts the scan task. The first day of the month is the default value.

- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **After application startup.** If this item is selected, Kaspersky Endpoint Security starts the scan task every time that Kaspersky Endpoint Security is started.

The **Start in** setting is available for this item. It specifies the interval (in minutes) since the startup of Kaspersky Endpoint Security after which Kaspersky Endpoint Security starts the scan task. The default value is 15 minutes.

- **After every update.** If this item is selected, Kaspersky Endpoint Security starts the scan task after each update.

Postpone running after application startup for

This setting specifies the time interval after the startup of Kaspersky Endpoint Security by which the start of the scan task is postponed.

Because a large number of processes start at operating system startup, it is convenient to start the scan task with a time delay after startup of Kaspersky Endpoint Security.

The default value is 15 minutes.

This setting is unavailable if the **After application startup** or **After every update** items are selected from the **Frequency** drop-down list.

Run skipped tasks

This check box enables / disables automatic startup of skipped scan tasks. For example, a scan task can be skipped if the computer was turned off when the scan task was set to start. If the check box is selected, Kaspersky Endpoint Security starts the skipped scan task as soon as it becomes possible.

If the check box is cleared, Kaspersky Endpoint Security does not run skipped scan tasks. Instead, it carries out the next scan task in accordance with the current schedule.

This setting is unavailable if the **Minutes**, **Hours**, **After application startup**, or **After every update** items are selected from the **Frequency** drop-down list.

This check box is cleared by default.

Run only when the computer is idle

This check box enables / disables a function that suspends the start of the scan task when computer resources are limited. Kaspersky Endpoint Security starts the scan task when the screensaver is on and the computer is locked.

This check box is cleared by default.

The **User** section contains settings for starting the scan task under an account that differs from the one under which you have logged in to the operating system.

Run task as

This check box enables / disables the use of an account, which differs from the one under which you have logged in to the operating system, for starting the scan task.

If the check box is selected, Kaspersky Endpoint Security starts the scan task with the rights of the user that is specified in the **Name** field. The option is available for starting the scan task of Kaspersky Endpoint Security both manually and by a schedule.

If the check box is cleared, Kaspersky Endpoint Security starts the scan task under the current account that you have used to log in to the operating system.

This check box is cleared by default.

Name

A field for entering the name of the account under which the scan task is to be started.

This setting is available if the **Run task as** check box is selected.

Password

Field for entering the password for the account that is entered in the **Name** field.

This setting is available if the **Run task as** check box is selected.

Scan scope window

In this window, the administrator can form the scope of the virus scan.

The following settings are available:

Add

Clicking this button opens the **Select scan scope** window. In this window, you can add objects to be scanned.

Edit

Clicking this button opens the **Select scan scope** window. In this window, you can edit the path to an object to scan.

This button is available if a non-default object has been selected from the list of objects to scan.

Delete

This button deletes the selected scan object from the list of objects to scan.

This button is available if a non-default object has been selected from the list of objects to scan.

Scan scope. A list of objects to be scanned by Kaspersky Endpoint Security when running a scan task. Objects within the scan scope can include the kernel memory, running processes, boot sectors, system backup, mail databases, hard drives, removable drives or network drives, a folder or file.

If the check box next to the name of an object within the scan scope is selected, Kaspersky Endpoint Security scans this object.

If an object within the scan scope is cleared, Kaspersky Endpoint Security temporarily excludes this object from the scan.

By default, check boxes are selected next to all objects that have been added, except the **My email** and **All network drives** objects.

Select scan scope window

In this window, the administrator can select an object to be added to the virus scan scope.

The following settings are available:

Object

This field displays the path to the scan object that is selected from the folder tree above. You can specify a hard drive or network drive, folder, file, or file name mask as an object to be scanned.

You can also enter the path to a scan object manually.

File name masks must be entered with full paths to objects. For example:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** – All files in the C:\dir\ folder.
- **C:\dir*.exe** – All files with the .exe extension in the C:\dir\ folder.
- **C:\dir*.ex?** – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- **C:\dir\test** – Only the file C:\dir\test.

Add

This button adds the path to the selected object to be scanned or the file name mask to the list of objects to be scanned in the **Scan scope** window.

Include subfolders

This check box enables / disables scanning of folders that are inside the selected folder. If a subfolder contains other child folders, they are scanned as well. Kaspersky Endpoint Security scans subfolders of all levels.

This check box is selected by default.

Custom Scan subsection

In the **Security level** section, you can select one of the three file security levels that have been created by Kaspersky Lab specialists, or configure file security level settings on your own. When deciding on a file security level, be sure to take working conditions and the current situation into account.

High

If the probability of computer infection is very high, select this file security level.

Kaspersky Endpoint Security scans all types of files. When scanning compound files, Kaspersky Endpoint Security also scans mail-format files.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists.

Kaspersky Endpoint Security scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects. Kaspersky Endpoint Security does not scan archives or installation packages.

The **Recommended** file security level is selected by default.

Low

The settings of this file security level ensure maximum scanning speed.

Kaspersky Endpoint Security scans only new or modified files with the specified extensions on all hard drives, removable drives, and network drives of the computer. Kaspersky Endpoint Security does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

This button opens the Custom Scan task settings window.

By default

This button sets the file security level to **Recommended**.

The **Action on threat detection** section lets you select the action that Kaspersky Endpoint Security performs if the Custom Scan task detects infected files.

Select action automatically

If this option is selected, Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. This action is **Select action: Disinfect. Delete if disinfection fails**.

Perform action: Disinfect. Delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

To select the **Perform action: Disinfect. Delete if disinfection fails** action, select the **Perform action** setting and select the **Disinfect** and **Delete if disinfection fails** check boxes.

This action is selected by default.

Perform action: Disinfect

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, Kaspersky Endpoint Security moves them to Quarantine.

To select the **Perform action: Disinfect** action, select the **Perform action** setting, select the **Disinfect** check box, and clear the **Delete if disinfection fails** check box.

Perform action: Delete

If this option is selected, Kaspersky Endpoint Security automatically deletes all infected or probably infected files that are detected.

To select the **Perform action: Delete** action, select the **Perform action** setting, clear the **Disinfect** check box, and select the **Delete** check box.

Perform action: Inform

If this option is selected, on detecting infected or probably infected files Kaspersky Endpoint Security informs you of this and moves the detected files to Quarantine.

To select the **Perform action: Inform** action, select the **Perform action** setting and clear the **Delete if disinfection fails** and **Disinfect** check boxes.

The **Run mode** section contains the settings that Kaspersky Endpoint Security uses to start the Custom Scan task.

Run mode

Clicking this button opens the **Run mode** tab in the **Custom Scan** window. This window lets you select the Custom Scan task run mode.

On the right of the button, the current task run mode is displayed.

Scope tab

The **File types** section lets you select the file types that Kaspersky Endpoint Security scans when performing the Custom Scan task.

Kaspersky Endpoint Security considers files without an extension as executable ones.
Kaspersky Endpoint Security always scans executable files regardless of the file types that you select for scanning.

All files

If this setting is enabled, Kaspersky Endpoint Security checks all files without exception (all formats and extensions).

This is the default setting.

Files scanned by format

If this setting is selected, Kaspersky Endpoint Security scans only potentially infectable files. Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file (for example, .txt, .doc, or .exe). During scanning, the extension of the file is also taken into account.

Files scanned by extension

If this setting is selected, Kaspersky Endpoint Security scans only potentially infectable files. The file format is then determined based on the file's extension.

Icon

Clicking the icon opens the Help system section of Kaspersky Endpoint Security. This section lists file extensions that are scanned by Kaspersky Endpoint Security.

The **Scan optimization** section contains settings that you can use to reduce the time that is needed to perform the Custom Scan task.

Scan only new and changed files

This check box enables / disables the mode of scanning only new files and files that have been modified since the previous scan. Kaspersky Endpoint Security scans both plain and compound files.

If the mode of scanning only new and modified files is enabled, the links for selecting scanning of all or only new files in the **Scan of compound files** section (**all / new**) become unavailable.

Skip files scanned longer than

The check box enables / disables the time duration for scanning an object. After the specified amount of time, Kaspersky Endpoint Security stops scanning a file.

File scanning is stopped by default after 30 seconds.

The **Scan of compound files** section contains a list of compound files that Kaspersky Endpoint Security scans for viruses and other threats.

Scan archives

This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

This check box is cleared by default.

The following scan options are available for archives:

- **All.** File Anti-Virus scans all archives.
- **New.** File Anti-Virus scans only new archives that have appeared after the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables / disables scanning of installation packages.

This check box is cleared by default.

The following scan options are available:

- **All.** File Anti-Virus scans all installation packages.
- **New.** File Anti-Virus scans only new installation packages that have appeared since the last scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan Office formats

This check box enables / disables the feature that File Anti-Virus uses during a virus scan to scan Office format files, including embedded OLE objects.

This check box is selected by default.

The following scan options are available:

- **All.** File Anti-Virus scans all Office format files.
- **New.** File Anti-Virus scans only new Office format files that have appeared since the time of the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Parse email formats

Scan password-protected archives

Additional

Compound files window

The **Size limit** section allows you to limit scanning of compound files that are of a specified size.

Do not unpack large compound files

If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the value that is specified in the **Maximum file size** field.

If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

Maximum file size

Kaspersky Endpoint Security does not unpack files, and only those files, that are larger than the specified value. The value is specified in megabytes.

Additional tab

The **Scan methods** section contains methods that Kaspersky Endpoint Security uses when scanning the computer.

Signature Analysis

Signature analysis uses the Kaspersky Endpoint Security database that contains descriptions of known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security.

Following the recommendations of Kaspersky Lab's experts, this method is always enabled.

Heuristic Analysis

This check box enables / disables Heuristic Analysis during scanning of the computer.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of detail of Heuristic Analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium scan** and **Deep scan** levels. Scanning is faster and less resource-intensive.

The **Light scan** detail level is set by default.

- **Medium scan.** While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
- **Deep scan.** While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

The **Scan technologies** section contains scan technologies that Kaspersky Endpoint Security uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. This speeds up anti-virus scanning of objects that are from various file systems and operating systems.

iSwift Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any changes made to the scan settings. The iSwift technology is an improvement on the iChecker technology for the NTFS file system.

The check box enables / disables the use of iSwift technology.

This check box is selected by default.

iChecker Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.

The check box enables / disables the use of iChecker technology.

This check box is selected by default.

Run mode tab

The **Run mode** section allows you to select the scan task run mode.

Manually

This scan task run mode allows you to start the scan task manually.

By schedule

In this scan task run mode, Kaspersky Endpoint Security starts the scan task in accordance with the schedule that you create. If this scan task run mode is selected, you can also start the scan task manually.

Frequency

The items in this drop-down list determine the start time of the scan task.

This setting is available if the **By schedule** scan task run mode is selected.

The following items are available from the **Frequency** drop-down list:

- **Minutes.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in minutes.

The **Run every N minutes** setting is available for this value. It specifies the interval between startups of the scan task, in minutes. The value cannot exceed 59 minutes. The default value is 5 minutes.

- **Hours.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in hours.

The **Run every N hours** setting is available for this item. It sets the interval between startups of the scan task, in hours. The value cannot exceed 23 hours. The default value is one hour.

- **Days.** If this item is selected, Kaspersky Endpoint Security starts the scan task with the set time interval. The interval between startups of the scan task is calculated in days.

The following settings are available for this item:

- **Run every.** The item specifies the interval between startups of the scan task, in days. The default value is one day.

The value cannot exceed 31 days.

- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **Every week.** If this item is selected, Kaspersky Endpoint Security starts the scan task on the specified days of the week.

The following settings are available for this item:

- **Start on.** The check boxes enable / disable startup of the scan task on the selected days of the week.
- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.

- **At a specified time.** If you select this item, Kaspersky Endpoint Security starts the scan task on the specified day and at the specified time.

The **Start date and time** setting is available for this item. It specifies the day and time at which Kaspersky Endpoint Security starts the scan task. The date is specified in DD / MM / YY format; the time is specified in HH:MM:SS format. By default, the current date is selected and the time is set to 0:00:00.

- **Every month.** If this item is selected, Kaspersky Endpoint Security starts the scan task once per month on the specified day and at the specified time.

The following settings are available for this item:

- **Run every N-th day of the month.** This setting specifies the day of the month on which Kaspersky Endpoint Security starts the scan task. The first day of the month is the default value.
- **Start time.** This setting specifies the time at which the scan task is started. By default, it is set to 00:00.
- **After application startup.** If this item is selected, Kaspersky Endpoint Security starts the scan task every time that Kaspersky Endpoint Security is started.

The **Start in** setting is available for this item. It specifies the interval (in minutes) since the startup of Kaspersky Endpoint Security after which Kaspersky Endpoint Security starts the scan task. The default value is 15 minutes.

- **After every update.** If this item is selected, Kaspersky Endpoint Security starts the scan task after each update.

Postpone running after application startup for

This setting specifies the time interval after the startup of Kaspersky Endpoint Security by which the start of the scan task is postponed.

Because a large number of processes start at operating system startup, it is convenient to start the scan task with a time delay after startup of Kaspersky Endpoint Security.

The default value is 15 minutes.

This setting is unavailable if the **After application startup** or **After every update** items are selected from the **Frequency** drop-down list.

Run skipped tasks

This check box enables / disables automatic startup of skipped scan tasks. For example, a scan task can be skipped if the computer was turned off when the scan task was set to start. If the check box is selected, Kaspersky Endpoint Security starts the skipped scan task as soon as it becomes possible.

If the check box is cleared, Kaspersky Endpoint Security does not run skipped scan tasks. Instead, it carries out the next scan task in accordance with the current schedule.

This setting is unavailable if the **Minutes**, **Hours**, **After application startup**, or **After every update** items are selected from the **Frequency** drop-down list.

This check box is cleared by default.

Run only when the computer is idle

This check box enables / disables a function that suspends the start of the scan task when computer resources are limited. Kaspersky Endpoint Security starts the scan task when the screensaver is on and the computer is locked.

This check box is cleared by default.

The **User** section contains settings for starting the scan task under an account that differs from the one under which you have logged in to the operating system.

Run task as

This check box enables / disables the use of an account, which differs from the one under which you have logged in to the operating system, for starting the scan task.

If the check box is selected, Kaspersky Endpoint Security starts the scan task with the rights of the user that is specified in the **Name** field. The option is available for starting the scan task of Kaspersky Endpoint Security both manually and by a schedule.

If the check box is cleared, Kaspersky Endpoint Security starts the scan task under the current account that you have used to log in to the operating system.

This check box is cleared by default.

Name

A field for entering the name of the account under which the scan task is to be started.

This setting is available if the **Run task as** check box is selected.

Password

Field for entering the password for the account that is entered in the **Name** field.

This setting is available if the **Run task as** check box is selected.

Starting or stopping a scan task

Regardless of the selected scan task run mode, you can start or stop a scan task at any time.

To start or stop a scan task:

3. Open the main application window.
4. Select the **Protection and Control** tab.
5. Click the **Tasks** section.

The **Tasks** section opens.

6. Right-click to bring up the context menu of the line with the scan task name.

A menu with scan task actions opens.

7. Do one of the following:

- If you want to start the scan task, select **Start scanning** from the menu.

The task progress status that is displayed on the right of the button with the name of this scan task changes to *Running*.

- If you want to stop the scan task, select **Stop scanning** from the menu.

The task progress status that is displayed on the right of the button with the name of this scan task changes to *Stopped*.

Starting or stopping an integrity check task

Regardless of the selected run mode, you can start or stop an integrity check task at any time.

► *To start or stop an integrity check task:*

8. Open the main application window.

9. Select the **Protection and Control** tab.

10. Open the **Tasks** section.

11. Right-click to bring up the context menu of the line with the integrity check task name.

12. Do one of the following:

- To start the integrity check task, select **Start scanning** from the context menu.

The task progress status that is displayed on the right of the button with the name of this task changes to *Running*.

- If you want to stop the integrity check task, select **Stop scanning** from the context menu.

The task progress status that is displayed on the right of the button with the name of this task changes to *Stopped*.

Managing Quarantine and Backup

This section describes how you can configure and manage Quarantine and Backup.

In this section:

About Quarantine and Backup

Configuring Quarantine and Backup settings

Managing Quarantine

Managing Backup

About Quarantine and Backup

Quarantine is a list of probably infected files. *Probably infected files* are files that may contain viruses and other threats, or varieties of such threats.

When Kaspersky Endpoint Security quarantines a probably infected file, it does not copy the file, but moves it: the application deletes the file from the hard drive or email message and saves the file in a special data storage. Files in Quarantine are saved in a special format and do not pose a threat.

Kaspersky Endpoint Security can detect and quarantine a probably infected file during a virus scan (see section "Scanning the computer" on page 199), and during the operation of File Anti-Virus (see section "About File Anti-Virus" on page 155), Mail Anti-Virus (see section "About Mail Anti-Virus" on page 173) and System Watcher (on page 194) protection components.

Kaspersky Endpoint Security places files in Quarantine in the following cases:

- File code resembles a known but partly modified malicious program, or has a malware-like structure, and is not listed in the Kaspersky Endpoint Security database. In this case, the file is placed in Quarantine after heuristic analysis by File Anti-Virus and Mail Anti-Virus, or during a virus scan. Heuristic analysis rarely causes false positives.
- The sequence of operations that a file performs is dangerous. In this case, the file is placed in Quarantine after the System Watcher component has analyzed its behavior.

Backup is a list of backup copies of files that have been deleted or modified during the disinfection process. *Backup copy* is a file copy created at the first attempt to disinfect or delete this file. Backup copies of files are stored in a special format and do not pose a threat.

Sometimes it is not possible to maintain the integrity of files during disinfection. If you partially or completely lose access to important information in a disinfected file after disinfection, you can attempt to restore the disinfected copy of the file to its original folder.

It is possible that, after another database or application software module update, Kaspersky Endpoint Security can definitely identify the threats and neutralize them. It is therefore recommended to scan quarantined files after each database and application software module update.

Configuring Quarantine and Backup settings

Data storage consists of Quarantine and Backup. You can configure Quarantine and Backup settings as follows:

- Configure the maximum storage term for files in Quarantine and file copies in Backup.

The default maximum storage term for files in Quarantine and file copies in Backup is 30 days. When the maximum storage term expires, Kaspersky Endpoint Security deletes the oldest files from the data storage. You can cancel the time-based restriction or change the maximum file storage term.

- You can configure the maximum size of Quarantine and Backup.

By default, the maximum Quarantine and Backup size is 100 MB. When data storage reaches its limit, Kaspersky Endpoint Security automatically deletes the oldest files from Quarantine and Backup so that the maximum data storage size is not exceeded. You can cancel the Quarantine and Backup size limit or change their maximum size.

In this section:

Configuring the maximum storage term for files in Quarantine and file copies in Backup

Configuring the maximum size of Quarantine and Backup

Configuring the maximum storage term for files in Quarantine and file copies in Backup

- *To configure the maximum storage term for files in Quarantine and file copies in Backup:*

13. Open the application settings window.

14. In the left part of the window, in the **Advanced settings** section, select **Reports and Storages**.

15. Do one of the following:

- To limit the Quarantine and Backup file storage term, in the **Quarantine and backup settings** section in the right part of the window, select the **Store objects no longer than** check box. In the field on the right of the **Store objects no longer than** check box, specify the maximum storage term for files in Quarantine and file copies in Backup. The storage term for files in Quarantine and file copies in Backup is limited to 30 days by default.
- To cancel the Quarantine and Backup file storage term limitation, in the **Quarantine and backup settings** section in the right part of the window, select the **Store objects no longer than** check box.

16. To save changes, click the **Save** button.

Configuring the maximum size of Quarantine and Backup

► *To configure the maximum Quarantine and Backup size:*

17. Open the application settings window.

18. In the left part of the window, in the **Advanced settings** section, select **Reports and Storages**.

19. Do one of the following:

- If you want to limit the total size of Quarantine and Backup, select the **Maximum storage size** check box in the right part of the window in the **Quarantine and Backup Settings** section and specify the maximum size of Quarantine and Backup in the field to the right of the **Maximum storage size** check box.

By default, the maximum storage size for data comprising the Quarantine directory and backup copies of files is 100 MB.

- If you want to remove the limit on the size of Quarantine and Backup, clear the **Maximum storage size** check box in the right part of the window in the **Quarantine and Backup Settings** section.

The size of Quarantine and Backup is unlimited by default.

20. To save changes, click the **Save** button.

Managing Quarantine

Kaspersky Endpoint Security automatically deletes files with any status from Quarantine after the storage term defined in the application settings has elapsed.

The following file operations are available when managing Quarantine:

- View the files that are quarantined by Kaspersky Endpoint Security.
- Scan probably infected files by using the current version of Kaspersky Endpoint Security databases and modules.

- Restore files from Quarantine to their original folders.
- Remove files from Quarantine.
- Open the folders where files were originally located.

The set of quarantined files is presented as a table.

You can also perform the following actions while managing data in the table:

- Filter quarantined files based on columns and custom filter conditions.
- Use the quarantined file search function.
- Sort quarantined files.
- Change the order and set of columns that are displayed in the table of quarantined files.

You can copy selected Quarantine events to the clipboard. To select multiple quarantined files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

In this section:

Enabling and disabling scanning of files in Quarantine after an update

Starting a Custom Scan task for files in Quarantine

Restoring files from Quarantine

Deleting files from Quarantine

Enabling and disabling scanning of files in Quarantine after an update

If Kaspersky Endpoint Security detects signs of infection when scanning a file but is unable to determine which specific malicious programs have infected it, Kaspersky Endpoint Security moves this file to Quarantine. Kaspersky Endpoint Security may definitely identify the threats and

neutralize them after the databases and application modules are updated. You can enable the automatic scanning of files in Quarantine after each update of the databases and application modules.

We recommend that you regularly scan files in Quarantine. Scanning may change the status of files. Some files can then be disinfected and restored to their original locations so that you can continue using them.

► *To enable scanning of quarantined files after updates:*

21. Open the application settings window.

22. In the left part of the window, in the **Advanced settings** section, select **Reports and Storages**.

In the right part of the window, the management settings for reports and storages are displayed.

23. In the **Quarantine and Backup Settings** section, do one of the following:

- To enable the scanning of quarantined files after each update of Kaspersky Endpoint Security, select the **Rescan Quarantine after update** check box.
- To disable the scanning of quarantined files after each update of Kaspersky Endpoint Security, clear the **Rescan Quarantine after update** check box.

24. To save changes, click the **Save** button.

Starting a Custom Scan task for files in Quarantine

After an update of databases and application software modules, Kaspersky Endpoint Security can definitely identify the threats in quarantined files and neutralize them. If the application is not configured to scan quarantined files automatically after each update of databases and application modules, you can manually start a Custom Scan task for quarantined files.

To start a Custom Scan task for quarantined files:

25. Open the main application window.

26. In the upper part of the main application window, click the **Quarantine** link to open the **Storages** window.

The **Quarantine** tab of the **Storages** window opens.

27. On the **Quarantine** tab, select one or more probably infected files that you want to scan.

To select multiple quarantined files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

28. Start the Custom Scan task in one of the following ways:

- Click the **Re-scan** button.
- Right-click to bring up the context menu and select **Rescan**.

When the scan is completed, a notification with the number of scanned files and the number of detected threats appears.

Restoring files from Quarantine

To restore files from Quarantine:

29. Open the main application window.

30. In the upper part of the main application window, click the **Quarantine** link to open the **Storages** window.

The **Quarantine** tab of the **Storages** window opens.

31. If you want to restore all quarantined files, select **Restore all** from the context menu of any file.

Kaspersky Endpoint Security restores all files from Quarantine to their original folders.

32. To restore one or more quarantined files:

- a. On the **Quarantine** tab, select one or more files that you want to restore from Quarantine.

To select multiple quarantined files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

b. Restore files in one of the following ways:

- Click the **Restore** button.
- Right-click to open the context menu and select **Restore**.

Kaspersky Endpoint Security restores the selected files to their original folders.

Deleting files from Quarantine

To delete files from Quarantine:

33. Open the main application window.

34. In the upper part of the main application window, click the **Quarantine** link to open the **Storages** window.

The **Quarantine** tab of the **Storages** window opens.

35. If you want to delete all files from Quarantine, select **Delete all** from the context menu of any file.

Kaspersky Endpoint Security deletes all files from Quarantine.

36. To delete one or more quarantined files:

- a. In the table on the **Quarantine** tab, select one or more probably infected files that you want to delete from Quarantine.

To select multiple quarantined files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

b. Delete files in one of the following ways:

- Click the **Remove** button.
- Right-click to open the context menu and select **Delete**.

Kaspersky Endpoint Security deletes the selected files from Quarantine.

Managing Backup

If malicious code is detected in the file, Kaspersky Endpoint Security blocks the file, places a copy of it in Backup, and attempts to disinfect it. If file disinfection succeeds, the status of the backup copy of the file changes to *Disinfected*. The file becomes available in its original folder. If a file cannot be disinfected, Kaspersky Endpoint Security deletes it from its original folder. You can restore the file from its backup copy to its original folder.

Upon detecting malicious code in a file that is part of the Windows Store application, Kaspersky Endpoint Security immediately deletes the file without moving a copy of the file to Backup. You can restore the integrity of the Windows Store application by using the appropriate tools of the Microsoft Windows 8 operating system (see the *Microsoft Windows 8 help files* for details on restoring a Windows Store application).

Kaspersky Endpoint Security automatically deletes backup copies of files with any status from Backup after the storage term defined in the application settings has elapsed.

You can also manually delete any copy of a file from Backup.

The set of backup copies of files is presented as a table.

While managing Backup, you can perform the following actions with backup copies of files:

- View the set of backup copies of files.
- Restore files from backup copies to their original folders.
- Delete backup copies of files from Backup.

You can also perform the following actions while managing data in the table:

- Filter backup copies by columns, including by custom filter conditions.
- Use the backup copy search function.
- Sort backup copies.

- Change the order and set of columns that are displayed in the table of backup copies.

You can copy selected Backup events to the clipboard. To select multiple Backup files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

In this section:

Restoring files from Backup

Deleting backup copies of files from Backup

Restoring files from Backup

► To restore files from Backup:

37. Open the main application window.

38. In the upper part of the main application window, click the **Quarantine** link to open the **Storages** window.

39. In the **Storages** window, select the **Backup** tab.

40. If you want to restore all files from Backup, select **Restore all** from the context menu of any file.

Kaspersky Endpoint Security restores all files from their backup copies to their original folders.

41. To restore one or more files from Backup :

c. In the table on the **Backup** tab, select one or multiple Backup files.

To select multiple quarantined files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

d. Restore files in one of the following ways:

- Click the **Restore** button.
- Right-click to open the context menu and select **Restore**.

Kaspersky Endpoint Security restores files from the selected backup copies to their original folders.

Deleting backup copies of files from Backup

► *To delete backup copies of files from Backup:*

42. Open the main application window.

43. In the upper part of the main application window, click the **Quarantine** link to open the **Storages** window.

44. In the **Storages** window, select the **Backup** tab.

45. If you want to delete all files from Backup, perform one of the following actions:

- In the context menu of any file, select **Delete all**.
- Click the **Clear storage** button.

Kaspersky Endpoint Security deletes all backup copies of files from Backup.

46. If you want to delete one or more files from Backup:

e. In the table on the **Backup** tab, select one or multiple Backup files.

To select multiple Backup files, right-click to open the context menu of any file and choose **Select all**. To deselect files that you do not want to scan, click them while holding down the **CTRL** key.

f. Delete files in one of the following ways:

- Click the **Remove** button.
- Right-click to open the context menu and select **Delete**.

Kaspersky Endpoint Security deletes the selected backup copies of files from Backup.

Working with encrypted devices when there is no access to them

Obtaining access to encrypted devices

A user may be required to request access to encrypted devices in the following cases:

- The hard drive was encrypted on a different computer.
- The encryption key for a device is not on the computer (for example, upon the first attempt to access the encrypted removable drive on the computer), and the computer is not connected to Kaspersky Security Center.

After the user has applied the access key to the encrypted device, Kaspersky Endpoint Security saves the encryption key on the user's computer and allows access to this device upon subsequent access attempts even if there is no connection to Kaspersky Security Center.

Access to encrypted devices can be obtained as follows:

1. The user uses the Kaspersky Endpoint Security application interface to create a request access file with the kesdc extension and sends it to the corporate LAN administrator.
2. The administrator uses the Kaspersky Security Center Administration Console to create an access key file with the kesdr extension and sends it to the user.
3. The user applies the access key.

Restoring data on encrypted devices

A user can use the Encrypted Device Restore Utility (hereinafter referred to as the "Restore Utility") to work with encrypted devices. This may be required in the following cases:

- The procedure for using an access key to obtain access was unsuccessful.
- Encryption components have not been installed on the computer with the encrypted device.

The data needed to restore access to encrypted devices using the Restore Utility resides in the memory of the user's computer in unencrypted form for some time. To reduce the risk of unauthorized access to such data, you are advised to restore access to encrypted devices on trusted computers.

Data on encrypted devices can be restored as follows:

1. The user uses the Restore Utility to create a request access file with the fdertc extension and sends it to the corporate LAN administrator.
2. The administrator uses the Kaspersky Security Center Administration Console to create an access key file with the fdertr extension and sends it to the user.
3. The user applies the access key.

To restore data on encrypted system hard drives, the user can also specify the Authentication Agent account credentials in the Restore Utility. If the metadata of the Authentication Agent account has been corrupted, the user must complete the restoration procedure using a request access file.

Before restoring data on encrypted devices, it is recommended to cancel the Kaspersky Security Center encryption policy on the computer where this operation is to be performed. This prevents the drive from being encrypted again.

In this section:

Obtaining access to encrypted devices through the application interface	257
Creating the executable file of Restore Utility	258
Restoring data on encrypted devices using the Restore Utility	259

Obtaining access to encrypted devices through the application interface

These instructions are intended for users of client computers with Kaspersky Endpoint Security installed.

► *To obtain access to encrypted devices through the application interface:*


1. Attempt to access the encrypted device that you need.

The **Access to data is blocked** window opens.

2. Send the corporate LAN administrator the request access file with the kesdc extension for the encrypted device. To do so, perform one of the following:
 - To email the corporate LAN administrator the generated request access file for the encrypted device, click the **Send by email** button.
 - To save the request access file for the encrypted device and deliver it to the corporate LAN administrator using a different method, click the **Save** button.

If you have closed the **Access to data is blocked** window without saving the request access file or without sending it to the corporate LAN administrator, you can do this at any time in the **Events** window on the **Status of access to files and devices** tab. To open this window, click the  button in the main application window.

3. Obtain and save the encrypted device access key file that has been created and provided to you by the corporate LAN administrator.
4. Use one of the following methods to apply the access key for accessing the encrypted device:
 - In any file manager, find the encrypted device access key file and double-click it to open it.
 - Do the following:

- a. Open the main window of Kaspersky Endpoint Security.
- b. Click the  button to open the **Events** window.
- c. Select the **Status of access to files and devices** tab.

The tab displays a list of all requests for access to encrypted files and devices.

- d. Select the request for which you received the access key file for accessing the encrypted device.
- e. To load the received access key file for accessing the encrypted device, click **Browse**.

The standard **Select access key file** Microsoft Windows dialog box opens.


- f. In the standard **Select access key file** window of Microsoft Windows, select the administrator-provided file with the kesdr extension and name matching the file name of the corresponding request access file for the encrypted device.
- g. Click the **Open** button.
- h. In the **Status of access to files and devices** window, click **OK**.

As a result, Kaspersky Endpoint Security grants access to the encrypted device.

Creating the executable file of Restore Utility

These instructions are intended for users of client computers with Kaspersky Endpoint Security installed.

► *To create the executable file of Restore Utility:*

1. Open the main application window.
2. Click the  button in the bottom left corner of the main application window to open the **Support** window.
3. In the **Support** window, click the **Restore encrypted device** button.

Encrypted device Restore Utility starts.

4. Click the **Create standalone Restore Utility** button in the window of Restore Utility.

The **Creating standalone Restore Utility** window opens.


5. In the **Save to** window, manually type the path to the folder for saving the executable file of Restore Utility, or click the **Browse** button.
6. Click **OK** in the **Creating standalone Restore Utility** window.

The executable file of Restore Utility (fdert.exe) is saved in the selected folder.

Restoring data on encrypted devices using the Restore Utility

These instructions are intended for users of client computers with Kaspersky Endpoint Security installed.

► To restore access to an encrypted device using the Restore Utility:

1. Run Restore Utility in one of the following ways:
 - Click the  button in the main window of Kaspersky Endpoint Security to open the **Support** window and click the **Restore encrypted device** button.
 - Run the executable file of Restore Utility fdert.exe. This file is created using Kaspersky Endpoint Security (see section "Creating the executable file of Restore Utility" on page [258](#)).
2. In the Restore Utility window, from the **Select device** dropdown list select an encrypted device to which you want to restore access.
3. Click the **Scan** button to allow the utility to define which of the actions should be taken on the device: whether it should be unlocked or decrypted.

If the computer has access to Kaspersky Endpoint Security encryption functionality, the Restore Utility prompts you to unlock the device. While unlocking the device does not decrypt it, the device becomes directly accessible as a result of being unlocked. If the

computer does not have access to Kaspersky Endpoint Security encryption functionality, the Restore Utility prompts you to decrypt the device.

4. Click the **Fix MBR** button if diagnostics of the encrypted system hard drive has returned a message about problems involving the master boot record (MBR) of the device.

Fixing the master boot record of the device can speed up the process of collecting information that is needed for unlocking or decrypting the device.

5. Click the **Unlock** or **Decrypt** button depending on the results of diagnostics.

The **Device unlock settings** or **Device decryption settings** window opens.

6. If you want to restore data using an Authentication Agent account:
 - g. Select the **Use Authentication Agent account settings** option.
 - h. In the **Name** and **Password** fields, specify the Authentication Agent account credentials.

This method is possible only when restoring data on a system hard drive. If the system hard drive was corrupted and Authentication Agent account data has been lost, you must obtain an access key from the corporate LAN administrator to restore data on an encrypted device.

7. If you want to use an access key to restore data:
 - i. Select the **Specify device access key manually** option.
 - j. Click the **Get access code** button.
 - k. The **Receive device access key** window opens.
 - l. Click the **Save** button and select the folder in which to save the request access file with the fdertc extension.
 - m. Send the request access file to the corporate LAN administrator.

Do not close the **Receive device access key** window until you have received the access key. When this window is opened again, you will not be able to apply the access key that was previously created by the administrator.

- n. Obtain and save the access key file that was created and provided to you by the corporate LAN administrator.
 - o. Click the **Load** button and select the access key file with the fdertr extension in the window that opens.
8. If you are decrypting a device, you must also specify the other decryption settings in the **Device decryption settings** window. To do so:
- Specify the area to decrypt:
 - If you want to decrypt the entire device, select the **Decrypt entire device** option.
 - If you want to decrypt a portion of the data on a device, select the **Decrypt individual device areas** option and use the **Start** and **End** fields to specify the decryption area boundaries.
 - Select the location for writing the decrypted data:
 - If you want the data on the original device to be rewritten with the decrypted data, clear the **Save data to file after decryption** check box.
 - If you want to save decrypted data separately from the original encrypted data, select the **Save data to file after decryption** check box and use the **Browse** button to specify the path in which to save the data.
9. Click **OK**.

The device unlocking / decryption process starts.

Using Authentication Agent

If system hard drives are encrypted, the Authentication Agent loads before startup of the operating system. Use the Authentication Agent to complete authentication for obtaining access to encrypted system hard drives and load the operating system.

After successful completion of the authentication procedure, the operating system loads. The authentication process is repeated every time the operating system restarts.

The user may be unable to pass authentication in some cases. For example, authentication is impossible if the user has forgotten the account credentials of the Authentication Agent account or the password to the token or smart card, or has lost the token or smart card.

If the user has forgotten the Authentication Agent account credentials or the password from a token or smart card, you must contact the corporate LAN administrator to recover them.

If a user has lost a token or smart card, the administrator must add the file of a token or smart card electronic certificate to the command for creating an Authentication Agent account. The user must then complete the procedure for restoring data on encrypted devices (see section "Working with encrypted devices when there is no access to them" on page [242](#)).

In this section:

Main window of Authentication Agent.....	262
Restoring Authentication Agent account credentials.....	263

Main window of Authentication Agent

In this window, the user must enter Authentication Agent account credentials to obtain access to an encrypted system hard drive and to load the operating system.

The following entry fields are available:

1. **Domain.**

In this field, you must enter the name of the domain in which the Authentication Agent account is registered.

2. **Login.**

In this field, you must enter the Authentication Agent account name.

3. **Password.**

In this field, you must enter the Authentication Agent account password.

In the lower part of the window, the following items are available to the user:

- Drop-down list for selecting the language of the Authentication Agent interface.
- Drop-down list for selecting the country.
- Button used to display the On-Screen Keyboard.
- Button used to display reference information about Authentication Agent.

If users forget their Authentication Agent account credentials, they can restore them by clicking the **Forgot your password** button. This starts the procedure for restoring account credentials (see section "Restoring Authentication Agent account credentials" on page [263](#)).

Restoring Authentication Agent account credentials

► *To restore Authentication Agent account credentials, the user of the client computer with an encrypted system hard drive must perform the following actions:*

1. Provide the request blocks generated by the application in Authentication Agent to the corporate LAN administrator.
2. Enter the request response blocks generated by the administrator in the Kaspersky Security Center Administration Console.
3. Enter a new password for the Authentication Agent account and confirm it.

The Authentication Agent account name is defined using the sections of the response to the requests for restoration of the Authentication Agent account credentials.

After you enter and confirm the new password of the Authentication Agent account, the password will be saved and you will be provided access to encrypted system hard drives.

In this section:

Step 1. Entropy	264
Step 2. Challenge.....	264
Step 3. Response.....	264

Step 1. Entropy

At this step, the user needs to randomly press keys on the keyboard or randomly move the mouse cursor so that the application can generate a random sequence of characters to strengthen the encryption algorithm.

Step 2. Challenge

At this step, the application generates blocks of the request to restore Authentication Agent account credentials. The user must communicate these blocks to the corporate LAN administrator and click **Continue**.

Step 3. Response

At this step, for each request block, the user must enter his or her block of the answer received from the corporate LAN administrator.

Remote administration of the application through Kaspersky Security Center

This section describes Kaspersky Endpoint Security administration through Kaspersky Security Center.

In this section:

About managing the application via Kaspersky Security Center	265
Managing policies	266
Tasks	489

About managing the application via Kaspersky Security Center

Kaspersky Security Center lets you remotely install and uninstall, start and stop Kaspersky Endpoint Security, configure application setting, change the set of available application components, add keys, and start update and scan tasks.

For additional information about managing the application via Kaspersky Security Center that is not provided in this document, please refer to the *Kaspersky Security Center Administrator's Guide*.

The application can be managed via Kaspersky Security Center using the Kaspersky Endpoint Security administration plug-in.

The version of the administration plug-in may differ from the version of Kaspersky Endpoint Security installed on the client computer. If the installed version of the administration plug-in has less functionality than the installed version of Kaspersky Endpoint Security, the settings of the missing functions are not regulated by the administration plug-in. These settings can be modified by the user in the local interface of Kaspersky Endpoint Security.

Managing policies

This section discusses the creation and configuration of policies for Kaspersky Endpoint Security. For more detailed information about managing Kaspersky Endpoint Security using Kaspersky Security Center policies, please refer to the *Kaspersky Security Center Administrator's Guide*.

In this section:



About policies.....	267
Application Startup Control.....	271
Application Privilege Control	283
Device Control	319
Web Control.....	344
Data encryption.....	376
Anti-Virus protection.....	401
Advanced application settings.....	467

About policies

You can use policies to apply identical Kaspersky Endpoint Security settings to all client computers within an administration group.

You can locally change the values of settings specified by a policy for individual computers in an administration group using Kaspersky Endpoint Security. You can locally change only those settings whose modification is not prohibited by the policy.

Whether an application setting on a client computer can be edited is determined by the "lock" status of the setting within a policy:

- If a setting is "locked" () , you cannot locally edit the value of this setting. The setting value specified by the policy is used for all client computers within the administration group.
- When a setting is "unlocked" () , you can edit the setting locally. A locally configured setting is applied to all client computers within the administration group. The policy-configured setting is not applied.

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

The rights to access policy settings (read, write, execute) are specified for each user who has access to the Kaspersky Security Center Administration Server and separately for each functional scope of Kaspersky Endpoint Security. To configure the rights to access policy settings, go to the **Security** section of the properties window of the Kaspersky Security Center Administration Server.

The following functional scopes of Kaspersky Endpoint Security are singled out:

- Anti-Virus protection. The functional scope includes File Anti-Virus, Mail Anti-Virus, Web Anti-Virus, IM Anti-Virus, Vulnerability Scan, and scan tasks.
- Application Startup Control The functional scope includes the Application Startup Control component.
- Device Control The functional scope includes the Device Control component.
- Encryption. The functional scope includes the hard drive, file, and folder encryption components.

- Trusted zone. The functional scope includes the Trusted Zone.
- Web Control The functional scope includes the Web Control component.
- Intrusion prevention. This functional scope includes Application Activity Monitor, Vulnerability Monitor, Firewall, Network Attack Blocker, and Application Privilege Control.
- Basic functionality. This functional scope includes general application settings that are not specified for other functional scopes, including: licensing, KSN settings, inventory tasks, application database and module update tasks, Self-Defense, advanced application settings, reports and storages, password protection settings, and application interface settings.

You can perform the following operations with a policy:

- Create a policy.
- Edit policy settings.

If the user account under which you accessed the Administration Server does not have rights to edit settings of certain functional scopes, the settings of these functional scopes are not available for editing.

- Delete a policy.
- Change policy status.

For information on using policies that are not related to interaction with Kaspersky Endpoint Security, please refer to the *Kaspersky Security Center Administrator's Guide*.

The General section

The **General** section contains the following policy information:

- Policy name (can be changed).
- Name of the application for which the policy has been created (for example, Kaspersky Anti-Virus 6.0 for Windows Workstations).

- Group of devices managed by the policy.
- Policy creation date and time.
- Date and time of the last modification of policy settings.

The **Enforcing the policy on devices** settings section also contains information about the results of policy application on the client devices within the selected group. The section indicates the number of devices on which the policy has the following statuses:

- *defined*
- *pending*
- *applied*
- *failed*

Event notification section

The **Event notification** section allows you to configure event logging and event notification. Events are distributed by importance level on the following tabs:

- Critical event
- Error
- Warning
- Info

The event list displays the names of events and the default event storage time on the Administration Server (in days). Clicking the **Properties** button lets you configure the settings of event logging and notifications about events selected in the list.

Application Startup Control

This section contains information about Application Startup Control and instructions on how to configure the component settings.

In this section:

About Application Startup Control	271
Application Startup Control subsection.....	271

About Application Startup Control

The Application Startup Control component monitors user attempts to start applications and regulates the startup of applications by using *Application Startup Control rules*.

Startup of applications whose settings do not match any of the Application Startup Control rules is regulated by the selected operating mode of the component. *Black List mode* is selected by default. This mode allows any user to start any application.

All user attempts to start applications are logged in reports.

Application Startup Control subsection

In this window, the administrator can perform the following tasks:

- Enable and disable Application Startup Control.
- Select the Application Startup Control mode - **Black list** or **White list**.
- Create Application Startup Control rules.
- Enable and disable control of DLL modules and drivers.
- Form templates for messages about events that occurred during the operation of Application Startup Control.

- View the list of applications installed on the computer.

The following settings are available:

Enable Application Startup Control

This check box enables / disables the Application Startup Control component.

When the check box is selected, Kaspersky Endpoint Security controls user attempts to start applications.

When the check box is cleared, Kaspersky Endpoint Security does not control user attempts to start applications.

This check box is cleared by default.

Application Startup Control mode

Items in this drop-down list define the operating mode of Application Startup Control.

You can choose one of the following items:

- **Black List**

If this item is selected, Application Startup Control allows all users to start any applications, except in cases when applications satisfy the conditions of Application Startup Control block rules.

- **White List**

If this item is selected, Application Startup Control blocks all users from starting any applications, except in cases when applications satisfy the conditions of Application Startup Control allow rules.

When this mode is selected, two Application Startup Control rules are created automatically:

- **Golden Image.**
- **Trusted updaters.**

The settings of these rules cannot be edited. You cannot delete these rules.

The **Black List** option is selected by default.

Action

Items in this drop-down list define the action to be performed by the component when a user attempts to start an application that is blocked by Application Startup Control rules.

You can choose one of the following items:

- **Block**

If this item is selected, when the user attempts to start an application that is blocked in the current mode of Application Startup Control, Kaspersky Endpoint Security blocks this application from starting. Information about the blocked application startup is logged in the report.

- **Notify**

If this item is selected, Kaspersky Endpoint Security allows the startup of the application that is blocked in the current mode of Application Startup Control, but logs information about its startup in the report.

The default option is **Block**.

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of the **Rule name**, **Allowed**, or **Blocked** columns of the Application Startup Control rule that you want to find in the table.

To view the search results in sequence, use the ◀ and ▶ buttons.

Add

Clicking this button opens the **Application Startup Control rule** window. You can create a new rule in this window.

Edit

Clicking this button opens the **Application Startup Control rule** window. You can edit the settings of the selected rule in this window.

The button is available if a rule to edit is selected from the list of rules.

Delete

This button deletes the selected rule.

The button is available if a rule is selected from the list of rules.

Application Startup Control rules

Table with a list of Application Startup Control rules.

The table contains the following columns:

- **Status.** This column displays the operating status of the rule:
 - **On.** This status means that the rule is used when Application Startup Control is in operation.

The check box selected next to the rule corresponds to this status.

- **Off.** This status means that the rule is ignored when Application Startup Control is in operation.

The check box cleared next to the rule corresponds to this status.

- **Rule name.** This column displays the name of the rule.
- **Allowed.** This column displays the names of users and / or user groups that are allowed to start applications that match the rule parameters.
- **Blocked.** This column displays the names of users and / or user groups that are prohibited from starting applications that match the rule parameters.

Monitor DLL and drivers

This check box enables / disables additional control over the loading of DLL modules.

If the check box is selected, Kaspersky Endpoint Security controls the loading of DLL modules when users attempt to start applications. Information about the DLL module and the application that loaded this DLL module is logged in the report.

If the check box is cleared, Kaspersky Endpoint Security does not control the loading of DLL modules when users attempt to start applications.

This check box is cleared by default.

Templates

This button opens the **Message templates** window. In this window, you can edit the message templates. These messages appear on the screen when Application Startup Control rules are triggered.

Application list

Clicking this button opens the **List of applications** window. This window lets you view the list of all applications that have been started on the computer since the installation of Kaspersky Endpoint Security.

Blockage tab

The entry field contains the template of the message that is displayed when an Application Startup Control rule that blocks an application from starting is triggered.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

Clicking this button opens a drop-down list that lets you insert a variable in the template text.

The following items are possible:

- **Name of the rule that has been applied (%RULE%).** The variable is replaced with the name of the Application Startup Control rule that blocked the application from starting.
- **Current date (%DATE%).** The variable is replaced with the date on which the application was blocked from starting, in DD.MM.YYYY format.

- **Current time (%TIME%).** The variable is replaced with the time when the application was blocked from starting, in HH:MM format.
- **User name (%USER_NAME%).** The variable is replaced with the name of the current account on the computer on which the application was blocked from starting.
- **Computer name (%COMPUTER_NAME%).** The variable is replaced with the name of the computer on which the application was blocked from starting.
- **Name of the executable file on the drive (%FILE_NAME%).** The variable is replaced with the name of the executable file of the blocked application.
- **KL category of the executable file (%KL_CAT%).** The variable is replaced with the name of the KL category to which Kaspersky Endpoint Security assigns the blocked application.
- **Path to executable file (%FILE_PATH%).** The variable is replaced with the path to the executable file of the blocked application.
- **Executable file version (%FILE_VERSION%).** The variable is replaced with the version of the executable file of the blocked application.
- **Original name of the executable file (%ORIGINAL_FILE_NAME%).** The variable is replaced with the original name of the executable file of the blocked application.
- **Vendor (%FILE_PUBLISHER%).** The variable is replaced with the name of the vendor of the blocked application.
- **Application name (%FILE_PRODUCT_NAME%).** The variable is replaced with the name of the blocked application.
- **Hash of the executable file (%FILE_MD5%).** The variable is replaced with the MD5 hash code of the executable file of the blocked application.
- **Certificate issuer (%CERT_ISSUER%).** The variable is replaced with the name of the issuer of the blocked application certificate.
- **Certificate subject (%CERT_SUBJECT%).** The variable is replaced with the subject of the certificate of the blocked application.

- **Certificate thumbprint (%CERT_THUMBPRINT%).** The variable is replaced with the thumbprint of the certificate of the blocked application.

Link. Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Message to administrator tab

The entry field contains the template of the user's message that is sent to the LAN administrator if the user believes that application startup has been blocked by mistake.

You can edit the text of the template.

To

Field for entering the email addresses to which messages should be sent to the LAN administrator.

Subject

Field for entering the subject of the message to the administrator.

The default subject is [Application Startup Control] Mistaken blocking.

By default

This button restores the original text of the template.

Variable

Clicking this button opens a drop-down list that lets you insert a variable in the template text.

The following items are possible:

- **Name of the rule that has been applied (%RULE%).** The variable is replaced with the name of the Application Startup Control rule that blocked the application from starting.
- **Current date (%DATE%).** The variable is replaced with the date on which the application was blocked from starting, in DD.MM.YYYY format.
- **Current time (%TIME%).** The variable is replaced with the time when the application was blocked from starting, in HH:MM format.

- **User name (%USER_NAME%).** The variable is replaced with the name of the current account on the computer on which the application was blocked from starting.
- **Computer name (%COMPUTER_NAME%).** The variable is replaced with the name of the computer on which the application was blocked from starting.
- **Name of the executable file on the drive (%FILE_NAME%).** The variable is replaced with the name of the executable file of the blocked application.
- **KL category of the executable file (%KL_CAT%).** The variable is replaced with the name of the KL category to which Kaspersky Endpoint Security assigns the blocked application.
- **Path to executable file (%FILE_PATH%).** The variable is replaced with the path to the executable file of the blocked application.
- **Executable file version (%FILE_VERSION%).** The variable is replaced with the version of the executable file of the blocked application.
- **Original name of the executable file (%ORIGINAL_FILE_NAME%).** The variable is replaced with the original name of the executable file of the blocked application.
- **Vendor (%FILE_PUBLISHER%).** The variable is replaced with the name of the vendor of the blocked application.
- **Application name (%FILE_PRODUCT_NAME%).** The variable is replaced with the name of the blocked application.
- **Hash of the executable file (%FILE_MD5%).** The variable is replaced with the MD5 hash code of the executable file of the blocked application.
- **Certificate issuer (%CERT_ISSUER%).** The variable is replaced with the name of the issuer of the blocked application certificate.
- **Certificate subject (%CERT_SUBJECT%).** The variable is replaced with the subject of the certificate of the blocked application.
- **Certificate thumbprint (%CERT_THUMBPRINT%).** The variable is replaced with the thumbprint of the certificate of the blocked application.

The method used to send messages and the utilized template depends on whether or not there is an active Kaspersky Security Center policy running on the computer that has Kaspersky Endpoint Security installed, and whether or not there is a connection with the Kaspersky Security Center Administration Server. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Security Center installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Security Center installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage. The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.
 - If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.
 - If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

Application Startup Control rule window

In this window, the administrator can create Application Startup Control rules.

An Application Startup Control rule contains the KL category used to create the rule, and the action performed by Application Startup Control when the rule is triggered (allowing or blocking application startup by users).

The administrator can perform the following actions on Application Startup Control rules:

- Add a new rule
- Modify the KL category based on which the rule was created.
- Edit rule status

An Application Startup Control rule can be enabled (the check box opposite the rule is selected) or disabled (the check box opposite the rule is cleared). An Application Startup Control rule is enabled by default after it is created.

- Delete rule

To work with Application Startup Control rules, the following settings are available:

Category

This drop-down list can be used to select an application category that was created previously. The rule controls the startup of applications that belong to the selected category.

The list does not display categories that were created based on the criterion of the MD5 hash of the executable file of the application.

Description

This field lets you describe an application or group of applications for which an Application Startup Control rule has been defined.

Principals and their rights

This table lets you specify users and/or user groups covered by the Application Startup Control rule.

The table contains the following columns:

- **Subject.** This column shows the users and/or user groups covered by the Application Startup Control rule.

The **Everyone** group is added by default. The rule applies to all users of a given computer.

- **Allow.** This column shows a check box that enables / disables permission to start applications that satisfy the rule conditions for users and/or user groups specified in the **Subject** column.

By default, the check box is cleared when the component runs in **Black list** mode and selected when the component runs in **White list** mode.

- **Deny.** This column shows a check box that enables / disables prohibition to start applications that satisfy the rule conditions for users and/or user groups specified in the **Subject** column.

By default, the check box is selected when the component runs in **Black list** mode and cleared when the component runs in **White list** mode.

Add

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window you can select the users and/or groups of users to be covered by the rule.

Delete

Clicking this button removes the selected user and/or user group from the **Principals and their rights** table. The component stops monitoring the startup of applications that satisfy the rule conditions by these users.

Deny for other users

Trusted updaters

The check box enables / disables the startup of applications which have been installed or updated by applications from the category that is specified in the rule, and for which no blocking rules are defined.

If the check box is selected, Kaspersky Endpoint Security considers applications that belong to the category that is specified in the rule to be trusted. Kaspersky Endpoint Security allows the startup

of applications which have been installed or updated by applications from the category that is specified in the rule if no blocking rules are defined for them.

By default, the check box is not selected.

Application Privilege Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Application Privilege Control and instructions on how to configure the component settings.

In this section:

About Application Privilege Control	283
Application Privilege Control subsection.....	284

About Application Privilege Control

Application Privilege Control prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources and to identity data.

This component controls the activity of applications, including their access to protected resources (such as files and folders, registry keys) by using *application control rules*. Application control rules are a set of restrictions that apply to various actions of applications in the operating system and to rights to access computer resources.

The network activity of applications is monitored by the Firewall component.

When an application is started for the first time, Application Privilege Control scans the application and places it in a trust group. A trust group defines the application control rules that Kaspersky Endpoint Security applies when controlling application activity.

We recommend that you participate in Kaspersky Security Network to make sure that Application Privilege Control is most effective. Data that is obtained through Kaspersky Security Network allows you to sort applications into groups with more accuracy and to apply optimum application control rules.

The next time the application starts, Application Privilege Control verifies the integrity of the application. If the application is unchanged, the component applies the current application control rules to it. If the application has been modified, Application Privilege Control re-scans it as if it were being started for the first time.

Application Privilege Control subsection

In this window, the administrator can perform the following tasks:

- Enable or disable Application Privilege Control.
- Configure rules for applications and protected resources.
- Configure the settings for assigning applications to trust groups.

The following settings are available:

Enable Application Privilege Control

This check box enables / disables operation of the Application Privilege Control component.

If the check box is selected, Application Privilege Control starts at Kaspersky Endpoint Security startup and registers the system activity of applications.

If the check box is cleared, Application Privilege Control is disabled.

This check box is selected by default.

Applications

This button opens the **Application control rules** tab in the **Application Privilege Control** window. This tab shows the list of applications access to which is monitored by Application Privilege Control. Applications are assigned to trust groups.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

Resources

This button opens the **Protected resources** tab in the **Application Privilege Control** window. This tab lets you view the list of personal data and operating system settings and resources to which Application Privilege Control controls access. You can also enable the protection of any resources in the list or add other resources to the list.

Update rules of previously unknown applications from KSN database

This check box enables / disables use of the Kaspersky Security Network database for updating the control rules for previously unknown applications.

If the check box is selected, Application Privilege Control updates the control rules for previously unknown applications by using the Kaspersky Security Network database.

This check box is selected by default.

Trust applications that have a digital signature

If this check box is selected, Application Privilege Control places digitally signed applications in the Trusted group.

If this check box is cleared, Application Privilege Control does not consider digitally signed applications to be trusted, and uses other parameters to determine their trust group.

This check box is selected by default.

Automatically move to group

If this option is selected, Application Privilege Control assigns an unknown application to the trust group that is selected in the **Low Restricted / High Restricted / Untrusted** drop-down list. The drop-down list is available if the **Automatically move to group** option is selected.

Use heuristic analysis to determine group

If this option is selected, Application Privilege Control uses heuristic analysis to determine the appropriate trust group for the unknown application.

This option is selected by default.

Maximum time to determine group

A field for entering the amount of time that is given to Application Privilege Control to heuristically analyze applications when they are started. The time period is specified in seconds.

By default, Application Privilege Control analyzes an application for 30 seconds. If Application Privilege Control cannot conclusively determine the danger rating of the application within this time, Application Privilege Control moves it to the "Low Restricted" trust group. Application Privilege Control continues to analyze the application in background mode and then assigns it to a specific trust group as determined through analysis.

Delete rules for applications that are not started for more than N days

This check box enables / disables the option to automatically delete application control rules for applications that have not been started for the specified time period. The time period is specified in days.

This check box is selected by default and Application Privilege Control deletes the control rules of applications that have not been started for more than 60 days.

Edit

Clicking this button opens the **Select trust group** window. This window lets you select a trust group according to whose rules the Firewall component will monitor the network activity of applications started before Kaspersky Endpoint Security.

Application control rules tab

In this window, the administrator can configure application control rules.

By default, application activity is controlled by application control rules that are defined for the trust group to which Kaspersky Endpoint Security assigned the application on first launch. If necessary, you can edit the application control rules for an entire trust group, for an individual application, or a group of applications that are within a trust group.

Application control rules that are defined for individual applications or groups of applications within a trust group have a higher priority than application control rules that are defined for a trust group. In other words, if the settings of the application control rules for an individual application or a group of applications within a trust group differ from the settings of application control rules for the trust group, the Application Privilege Control component controls the activity of the application or the group of applications within the trust group according to the application control rules that are for the application or the group of applications.

To create and modify application control rules, the following settings are available:

Application control rules

A table of control rules for applications that are categorized into trust groups. Kaspersky Endpoint Security follows the application control rules in regulating application access to operating system processes and resources.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,

- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is lower than 50,
- the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.






Such applications are subject to high restrictions on access to operating system resources.

You can sort the list of application control rules by trust group.

The context menu is available by right-clicking any column for the selected group of applications. From the context menu, you can do the following:

- Go to the application control rules or application group control rules.
- Create a subgroup within the application group.
- Restore the original settings of an application or group of applications (including all nested groups and applications).
- Delete an application or group of applications (not available for trust groups). When an application or group of applications is removed, the rules for this application or group of applications are removed from the table, and the Application Privilege Control and File Anti-Virus components no longer control the file and network activity of this application or of applications belonging to this group.
- Move an application to another trust group.

The table contains the following columns:

- **Application.** This column displays the names of the trust groups together with the applications and application groups assigned to them.
- **Vendor.** This column shows the name of the application vendor.
- **Group.** This column shows the icon of the trust group to which Application Privilege Control or the user has assigned the application:
 - Icon . Trusted.
 - Icon . Low Restricted.
 - Icon . High Restricted.
 - Icon . Untrusted.
 - Icon . The settings of the application control rule have been modified by the user.
- **Popularity.** This column shows the number of Kaspersky Security Network members that use this application.

Edit

This button opens the **Application control rules** or **Application group control rules** window. You can edit application control rules or application group control rules in this window.

This button is available when an application or group of applications is selected in the **Application control rules** table.

In the section located in the lower part of the window, you can view application details and change its trust group. This section is available when an application is selected in the list.

Group: Trusted / Low Restricted / High Restricted / Untrusted

The link designates the trust group to which the application is assigned.

Click the link to open the context menu. In the context menu, you can select a different trust group for this application. After you change the trust group, the application is automatically moved to the selected trust group in the list of application control rules.

Additional

Clicking the button opens the **Application control rules** window. This window lets you configure the rights of application access to monitored operating system resources and configure the network rules of this application.

File tab

In this window, you can view the following information about the executable file of an application:

Path

Path to the executable file of an application.

Vendor

Application vendor.

Application

Application name.

Product version

Version number of the installed application.

Size

Size of the executable file of the application.

Created

Application executable file creation date and time.

Modified

Application executable file modification date and time.

Status / Group

Trust group to which the application has been assigned by Kaspersky Endpoint Security or the user.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is lower than 50,
 - the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 51-71 range,
 - the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:
 - applications are not digitally signed by trusted vendors,
 - applications are not recorded in the trusted applications database of Kaspersky Security Network,
 - the threat index of applications is in the 71-100 range,
 - the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

Certificate status

Status of the certificate of a monitored application.

This information is available when the application is digitally signed.

The following setting values are possible:

- **Corrupted**
- **Revoked**
- **Untrusted.**
- **Expired**

- **Trusted (not verified)**
- **Trusted (verified)**
- **Absent**
- **Scan error**

Vendor

Certificate issuer.

Signature date

Digital signature creation date and time. This field is available when a digital signature exists.

Popularity

Number of users that use the application (based on the data that is received from Kaspersky Security Network).

Appeared in KSN

Date and time when the application first appeared on the computer of a Kaspersky Security Network participant.

Files and system registry tab

In this window, the administrator can configure the access of the selected application to files of the user and the operating system, and to the system registry.

The following settings are available:



Files and system registry

This table contains the rights of an application or application group to access operating system resources and identity data, which are combined into the **Files and system registry** category.

Operating system resources include system files, security settings, and various system services. They are combined into the **Operating system** category.

Personal data of the user includes user files and custom settings of applications. They are combined into the **Personal data** category.

Depending on whether or not the window has been opened from the context menu of the application or group of applications, the table lists the privileges of the application or application group to access operating system resources.

Access rights in the table are combined into groups that are presented hierarchically. You can display or hide entries of any group by clicking the  и  icons in the group header.




The table contains the following columns:

- **Resource.** This column shows the rights of an application or application group to access operating system resources and personal data of the user.

Entries in this column are sorted alphabetically by default. Groups and entries within each group are sorted alphabetically. A context menu in the column header lets you right-click to change the order of groups and entries within each group:

- **Sort ascending.** Selecting this command causes groups and values within each group to be sorted alphabetically.
- **Sort descending.** Selecting this command causes groups and values within each group to be sorted in reverse alphabetical order.
- **Read.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to read operating system resources and personal data of the user.
- **Write.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to modify and save existing resources of the operating system and personal data of the user.
- **Delete.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to delete operating system resources and personal data of the user.
- **Create.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to create and save new resources of the operating system and personal data of the user.

In the **Read**, **Write**, **Delete**, and **Create** columns, the selected right has a context menu that lets you right-click to modify the Kaspersky Endpoint Security action:

- The **Inherit** item signifies that the application or application group inherits the action of Kaspersky Endpoint Security from its parent group of rights. The displayed icon is identical to that of the parent group of rights.
- The  icon signifies that Kaspersky Endpoint Security allows the application or application group to access a process or resource of the operating system.
- The  icon signifies that Kaspersky Endpoint Security blocks the application or application group from accessing a process or resource of the operating system.
- The  icon signifies that, besides taking the specified action, Kaspersky Endpoint Security logs information about the attempt by an application or application group to access a process or resource of the operating system.



Rights tab

In this window, the administrator can configure the rights of the selected application to make modifications to the operation of the operating system.

The following settings are available:

Rights

This table lists the privileges of an application or group of applications to access processes and operating system resources depending on whether or not the window has been opened from the context menu of the application or group of applications.

Access rights in the table are combined into groups that are presented hierarchically. You can display or hide entries of any group. You can display entries of a group by clicking the  icon in the header of the group. You can hide entries of a group by clicking the  icon in the header of the group.

The table contains the following columns:

- **Resource.** This column displays the right of an application or application group to access processes and resources of the operating system.

Entries in this column are sorted alphabetically by default. Groups and entries within each group are sorted alphabetically. A context menu in the column header lets you right-click to change the order of groups and entries within each group:

- **Sort ascending.** Selecting this command causes groups and values within each group to be sorted alphabetically.
- **Sort descending.** Selecting this command causes groups and values within each group to be sorted in reverse alphabetical order.
- **Permission.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to access processes and resources of the operating system.

In this column, the selected right has a context menu that lets you right-click to modify the Kaspersky Endpoint Security action:

- The **Inherit** item signifies that the application or application group inherits the action of Kaspersky Endpoint Security from its parent group of rights. The displayed icon is identical to that of the parent group of rights.
- The  icon signifies that Kaspersky Endpoint Security allows the application or application group to access a process or resource of the operating system.
- The  icon signifies that Kaspersky Endpoint Security blocks the application or application group from accessing a process or resource of the operating system.
- The  icon signifies that, besides taking the specified action, Kaspersky Endpoint Security logs information about the attempt by an application or application group to access a process or resource of the operating system.

Network rules tab

In this window, the administrator can create network activity monitor rules for applications.

The following actions are available while managing application network rules:

- Create a new network rule.

The administrator can create a new network rule by which the Firewall must regulate the network activity of the application or applications that belong to the selected group of applications.

- Enable or disable a network rule.

All network rules are added to the list of network rules of applications with *Enabled* status. If a network rule is enabled, Firewall applies this rule.

The administrator can disable a network rule that was manually created. If a network rule is disabled, Firewall temporarily does not apply this rule.

- Change the settings of a network rule.

After the administrator creates a new network rule, he or she can always return to its settings and modify them as needed.

- Change the Firewall action for a network rule.

In the list of network rules, the administrator can edit the action that the Firewall applies for the network rule upon detecting network activity of this application or application group.

- Change the priority of a network rule.

The administrator can raise or lower the priority of a custom network rule.

- Delete a network rule.

The administrator can delete a custom network rule to stop the Firewall from applying this network rule to the selected application or application group upon detecting network activity, and to stop this rule from being displayed in the list of application network rules.

To work with network rules, the following settings are available:

Add

This button opens the **Network rule** window. You can create a new network rule in this window.

Edit

This button opens the **Network rule** window. You can edit the settings of the network rule in this window.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Delete

This button causes Firewall to delete the network rule that you select.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Firewall assigns an execution priority to each network rule. The priority of a network rule is determined by its position on the list of network rules. The topmost network rule in the list of network rules has the highest priority. Firewall processes network rules in the order in which they appear in the list of network rules, from top to bottom. Firewall locates the topmost rule that applies to the given network connection and executes it by either allowing or blocking network access.

Firewall ignores all subsequent network rules.

Move up

Clicking the button causes Firewall to move the selected network rule one line higher up on the list, thus increasing the rule's priority.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.

Move down

Clicking the button causes Firewall to move the selected network rule one line lower on the list, thus decreasing the rule's priority.

This button is unavailable for preset network rules that are specified by Firewall by default.

This button is available when a custom network rule is selected in the **Network rules** table.



Network rules

This table contains information about network rules of an application or application group. In accordance with these rules, Firewall regulates the network activity of an application or application group.

The table shows information about application network rules, if the window is opened from the context menu of the application. Application network rules are used for imposing network activity restrictions on a specific application. They factor in not only the characteristics of the network packet, but also the specific application to which this network packet is addressed or which issued this network packet. Such rules make it possible to fine-tune network activity filtering: for example, when a certain type of network connection is blocked for some applications but is allowed for others.

The table shows information about network rules of the application group, if the window is opened from the context menu of the application group. application group network rules have the same set of network activity restrictions that network rules for an application have. Firewall uses application group network rules for filtering the network activity of all applications within this group.

The table displays pre-configured network rules that are recommended by Kaspersky Lab for optimum protection of the network traffic of computers that run on Microsoft Windows operating systems. Such network rules are colored gray. The **Edit**, **Delete**, **Move up**, and **Move down** buttons are not available for them.

Some table columns include nested columns. You can open nested columns by clicking the  icon in the column header. You can hide nested columns by clicking the  icon in the column header.

The table contains the following columns:

Network service

The column contains a check box and name of the network service (value in the nested **Name** column). A *network service* is a collection of settings which describe the network activity for which you create a network rule.






The check box enables / disables the use of network rule.

When the check box is selected, Firewall applies this network rule.

When the check box is cleared, Firewall temporarily does not apply this network rule.

This column contains seven nested columns:

- **Name.** This column shows the name of a network service.
- **Direction.** This column shows an icon that indicates the direction of monitored network activity. The following network traffic directions are possible:



- Icon  – inbound. Firewall applies a network rule to a network packet or data stream that is received by the user's computer.
- Icon  – inbound (packet). Firewall applies the network rule to a network connection that is initiated by a remote computer.
- Icon  – inbound / outbound. Firewall applies the network rule to both inbound and outbound network packets or data streams, regardless of whether the user's computer or a remote computer initiated the network connection.
- Icon  – outbound. Firewall applies a network rule to a network packet or data stream that leaves the user's computer.
- Icon  – outbound (packet). Firewall applies the network rule to a network connection that is initiated by the user's computer.
- **Protocol.** This column shows the type of protocol for which Firewall monitors network connections.
- **Remote ports.** This column shows numbers of network ports of the remote computer.
- **Local ports.** This column shows numbers of network ports of the user's computer.
- **Network adapters.** This column shows the name of the adapter through which network traffic passes.
- **TTL.** This column shows the maximum time to live of outbound and/or inbound network packets that is specified in the network rule. A network rule controls the transmission of network packets whose time to live does not exceed the specified value.

Permission

This column shows the Firewall response on detecting network activity of an application or an application group that is subject to a network rule.

In this column, the selected network rule has a context menu. Right-click to bring it up and modify the Firewall action.

- The  icon signifies that Firewall allows access to the network resource.

- The  icon signifies that Firewall blocks access to the network resource.
- The  icon signifies that, besides taking the specified action, Firewall logs information about the attempt to access a network resource.

Address

This column shows the status of the network connection for which Firewall applies a network rule (the value of the nested **Remote addresses** column).

Firewall automatically detects the *network connection status* by analyzing network parameters. Depending on the network connection status, Firewall applies a set of network rules that are used for filtering network activity.

The network connection can have one of the following status types:

- **Public network.** This status is for networks that are not protected by any anti-virus applications, firewalls, or filters (for example, for Internet cafe networks). For the user of a computer that is connected to such a network, Firewall blocks access to files and printers of this computer. External users are also unable to access data through shared folders and remote access to the desktop of this computer. Firewall filters the network activity of each application according to the network rules that are set for it.

Firewall assigns *Public network* status to the Internet by default. You cannot change the status of the Internet.

- **Local network.** This status is assigned to networks whose users are trusted to access files and printers on this computer (for example, a LAN or home network).
- **Trusted network.** This status is intended for a safe network in which the computer is not exposed to attacks or unauthorized data access attempts. For networks with this status, Firewall permits any network activity within the given network.

This column contains two nested columns:

- **Local addresses.** This column does not contain any values because the **Local address** setting is not used when creating an application network rule or application group.
- **Remote addresses.** The column contains remote network addresses.

If the selected network rule is preset, the network rule settings are available for viewing only.

If the selected network rule is not preset, the network rule settings are displayed as links. Clicking any link opens the **Network rule** window, in which you can edit the network rule settings.

History tab

In this window, the administrator can view the history of application processing by Application Privilege Control.

The following information is available:

History

This table lists events or activities that occurred while access by applications or their child processes to operating system resources was monitored. Each line in the list of events contains information about the application or process and the action that was taken by Kaspersky Endpoint Security in response to an attempt by this application or process to access operating system resources.

You can filter the list of events by specifying the necessary filtering conditions:

- Clicking the icon in the header of any column opens a context menu with a list of filtering conditions. You can specify the following filtering conditions for this column:
 - **(Custom)**. Selecting this item opens the **Custom filter** window. This window lets you specify a custom event filtering condition.
 - **(All)**. In selecting this item, you specify a filtering condition whereby event entries with any attribute values are displayed in the list.
 - **<Attribute value>**. By selecting one of the attribute values, you specify a filtering condition whereby the list of events displays only event entries that have the specified attribute value.

After you select a filtering condition, the list of events is refreshed and displays only those entries that match the filtering condition.



- Right-clicking the header of any column opens a context menu that lets you select the **Filter** command. Selecting this item opens the **Custom filter** window that lets you specify a custom event filtering condition.

- Right-clicking the header of any column opens a context menu that lets you specify the composition of columns to display in the list of events.
 - When the check box next to the column name is selected, this column is displayed in the list of events.
 - When the check box next to the column name is cleared, this column is hidden in the list of events.

You can sort the list of events by any column, by specifying the necessary sorting method. By default, the list of events is sorted in ascending order of values in the **Event date** column. For this column, an event with a later logging time is considered to have a greater value.

The header of each column has a context menu that lets you right-click to change the order of events:

- **Sort ascending.** Selecting this command causes values in any column, except the **Event date** column, to be sorted alphabetically. The values in the **Event date** column are sorted in ascending order.
- **Sort descending.** Selecting this command causes values in any column, except the **Event date** column, to be sorted in reverse alphabetical order. The values in the **Event date** column are sorted in descending order.

Some table columns include nested columns. You can open nested columns by clicking the  icon in the column header. You can hide nested columns by clicking the  icon in the column header.

The table consists of the following columns:

Event date

This column shows the event logging date and time.

Application

This column contains six nested columns:

- **Name.** This column shows the name of the executable file of the application.
- **Path.** This column shows the full path to the executable file of the application.

- **Process ID.** This column shows the unique process ID that the operating system assigns on application startup.
- **Parameters.** This column shows the initial parameters of the application.
- **Module.** This column shows the name of the dll module that made a call to the function to which a Kaspersky Endpoint Security task or component responded.
- **Function.** The name of a function of a third-party application to which a Kaspersky Endpoint Security task or component responded.

Component

This column shows the name of the component that processes the event.

Result

This column contains five nested columns:

- **Description.** This column describes the decision or action of the component at the time of the event.
- **Type.** This column indicates the type of data that is handled by the component at the time of the event.
- **Name.** This column shows the action requested by the object, the link, or path to the object that is handled by the component at the time of the event.
- **Threat level.** This column shows the threat level based on which the component makes a decision to handle the event.
- **Precision.** This column reflects the accuracy of the event-handling decision that is made by the component.

Action

This column reflects the action that is taken by the component at the time of handling the event.

Object

This column shows the name of the object on which the action is taken at the time of handling the event (combined values of the **Path** and **Name** columns). This column contains three nested columns:

- **Type.** This column indicates the type of object on which the action is taken at the time of the event.
- **Path.** This column indicates the location of the object on which the action is taken at the time of the event.
- **Name.** This column indicates the name of the object on which the action is taken at the time of the event.

Reason

This column indicates the reason for the result of event processing.

Exclusions tab

In this window, the administrator can exclude certain actions of the selected application from the application control rules.

The following settings are available:

Do not scan opened files

This check box enables / disables the exclusion of all files opened by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan the files that the application opens.

Do not monitor application activity

This check box enables / disables the monitoring of file and network activity of an application in the operating system by the Application Privilege Control, System Watcher, and Firewall components.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of the application.

Do not inherit restrictions of the parent process (application)

This check box enables / disables inheritance by the application of application control rules and application network rules that are specified for the parent process (application).

If the check box is selected, Kaspersky Endpoint Security monitors application activity according to the rules that are specified by the system administrator: file activity is monitored according to application control rules, while network activity is monitored according to application network rules.

If the check box is cleared, Kaspersky Endpoint Security monitors application activity according to application control rules and the application network rules that are inherited from the parent process (application).

Do not monitor child application activity

This check box enables / disables the monitoring of file and network activity of any child application of this application.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of child applications of this application.

Do not block interaction with the application interface

The check box enables / disables permission for the application to interact with the Kaspersky Endpoint Security interface.

If the check box is selected, the remote access application is allowed to manage Kaspersky Endpoint Security settings through the Kaspersky Endpoint Security interface.

Do not scan network traffic

This check box enables / disables the exclusion of network traffic generated by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan incoming and outgoing traffic of this application according to the network traffic exclusion settings. You can configure the exclusion settings in the section that is below the **Do not scan network traffic** setting.

In the section below the **Do not scan network traffic** setting, you can edit the settings of network traffic exclusion from virus scanning.

The section is available if the **Do not scan network traffic** check box is selected.

Any / specified remote IP addresses

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote IP addresses.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote IP addresses.

Clicking the **specify** link opens the **Remote IP addresses** window. This window lets you specify the list of IP addresses that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

Any / specified remote ports

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote ports.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote ports.

Clicking the **specify** link opens the **Remote ports** window. This window lets you specify the list of remote ports that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

Protected resources tab

In this window, the administrator can configure application rights to access various categories of operating system resources and personal data.

Kaspersky Lab specialists have established preset categories of protected resources. The administrator cannot edit or delete the preset categories of protected resources or the protected resources that are within these categories.

The administrator can perform the following actions:

- Add a new category of protected resources.
- Add a new protected resource.
- Disable protection of a resource.

The following settings are available:

Exclusions

Clicking the button opens the **Exclusions** window. This window lets you form a list of computer resources to which Application Privilege Control does not control access.

Search field

In the search field, you can type the entire contents or any number of characters from the contents of the **Protected resources** table columns. The search starts as you enter characters.

To reset the search results, delete the contents of the search field.

Everywhere / By application names / By resource names

The items in this drop-down list specify the scope of search in the table of applications and protected resources:

- **Everywhere.** If this item is selected, the search includes the contents of all columns in the **Protected resources** table.
- **By application names.** If this element is selected, the search is conducted in the contents of the **Application** column of the **Protected resources** table.
- **By resource names.** If this item is selected, the search includes the contents of the left part of the **Protected resources** table.

Add

Clicking this button opens a list.

The drop-down list includes the following items:

- **Category.** Selecting this item opens the **Category of protected resources** window. In this window you can enter the name of a category of protected resources to be added to the **Protected resources** table.
- **File or folder / Registry key.** Selecting this item opens the **Protected resource** window. This window lets you specify the settings of the resource that is being added to the **Protected resources** list.

Edit

This button opens the **Category of protected resources** or the **Protected resource** window. These windows let you edit the name of a category of protected resources or the settings of a resource that is added to the **Protected resources** table.

This button is available when a category of protected resources or a protected resource is selected in the **Protected resources** table.

You cannot modify the default category of protected resources or default protected resources.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete the category of protected resources or resource selected in the **Protected resources** table.

You cannot delete the default category of protected resources or default protected resources.

Update

Clicking this button sends a query to the Administration Server to update the list of protected resources.

This button is available only in the Administration Console of Kaspersky Security Center.

Protected resources

The list contains categorized computer resources. Application Privilege Control monitors attempts by other applications to access resources in the list.

A resource can be a category, file or folder, or registry key.

If the check box next to a resource is selected, Application Privilege Control protects the resource.

If the check box next to a resource is cleared, Application Privilege Control temporarily excludes it from the protection scope.

Rules of application access to protected resources

A table with rules defining the access of applications or groups of applications to protected resources.

The table contains the following columns:




- **Application.** This column displays the names of the trust groups together with the applications and application groups assigned to them. For these applications you can configure the rules of access to protected resources in the list on the left. The rule settings (read, write, delete, create) configured for a protected resource within a group apply to the entire group of protected resources.

You can sort the list of application control rules by values in this column. Besides trust groups, the elements that they contain (application groups and applications within each group) are also sorted. To sort the list of application control rules by values in this column, right-click to display the context menu of the appropriate column header and use the following commands:

- **Sort ascending.** Selecting this command causes the list of application control rules to be sorted by the **Application** column values in strict alphabetical order.
- **Sort descending.** Selecting this command causes the list of application control rules to be sorted by the **Application** column values in reverse alphabetical order.
- **Read.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or group of applications to read protected resources.
- **Write.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or group of applications to modify and save protected resources.
- **Delete.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or group of applications to delete protected resources.
- **Create.** This column shows the Kaspersky Endpoint Security action that defines the right of an application or application group to create and save new resources of the operating system and personal data of the user.

In the **Read**, **Write**, **Delete**, and **Create** columns, the selected right of access for an application or group of applications has a context menu that lets you right-click to modify the Kaspersky Endpoint Security action:

- The **Inherit** item signifies that the application or application group inherits the action of Kaspersky Endpoint Security from its parent group of rights. The displayed icon is identical to that of the parent group of rights.

- The  icon signifies that Kaspersky Endpoint Security allows the application or group of applications to access a group of protected resources.
- The  icon signifies that Kaspersky Endpoint Security blocks the application or group of applications from accessing a group of protected resources.
- The  icon signifies that, besides taking the specified action, Kaspersky Endpoint Security logs information about the attempt by an application or group of applications to access a group of protected resources.

The access right configured for a protected resource within a group applies to the entire group of protected resources.

Exclusions window

In this window, the administrator can form a list of exclusions. Access to resources added to the list of exclusions is not monitored by Application Privilege Control components. A file, folder, or registry key can be specified as a resource.

The following settings are available:

Exclusions

The table lists resources that have been excluded by the user from the protection scope of Application Privilege Control. A resource can be a file, folder, or registry key.

Resources that are added to the list of exclusions by default cannot be edited or deleted.

If the check box next to a resource is selected, Application Privilege Control does not control access to this resource.

If the check box next to a resource is cleared, Application Privilege Control protects the resource.

The table contains the following columns:

- **Resource.** This column shows the resource name.
- **Path.** This column shows the path to the resource.

The path may contain a mask.

Add

This button opens a context menu. You can select the type of resource in the context menu: file or folder or registry key. When a context menu item is selected, the **Protected resource** window opens. This window lets you specify the settings of the resource that is being added to the **Exclusions** list.

Edit

This button opens the **Protected resource** window. This window lets you modify the settings of the resource that is being added to the **Exclusions** list.

This button is available if an item is selected in the **Exclusions** list.

Delete

This button causes Kaspersky Endpoint Security to remove the selected item.

This button is available if an item is selected in the **Exclusions** list.

Protected resource window

In this window, the administrator can select a protected resource.

The following settings are available:

Name

Field for entering the name of a resource access to which should be protected by Application Privilege Control.

Path

Field that shows the path to a file or folder that is selected for addition to the list of protected resources.

This field is available when you add a file or folder as a protected resource.

Registry path

Field that shows the path in the registry tree to the registry key that is selected for addition to the list of protected resources.

The field is available when you add a registry key as a protected resource.

Browse

Clicking this button opens a window. In this window you can select a file or folder, registry key or network service, or create a list of IP addresses for addition to the list of protected resources.

Select file or folder window

In this window, the administrator can select a protected resource.

The following settings are available:

Object

Field that displays the path to the file or folder that is selected in the above folder tree.

You can also type the path to a file or folder manually.

Only file name masks with full paths to files can be entered. For example:

- C:\dir*. * or C:\dir* or C:\dir\ – All files in the C:\dir\ folder.
- C:\dir*.exe – All files with the .exe extension in the C:\dir\ folder.
- C:\dir*.ex? – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- C:\dir\test – Only the file C:\dir\test.

Select registry object window

In this window, the administrator can select a protected resource.

The following settings are available:

Key

Field that shows the path to the registry key that is selected in tree mentioned above. You can type the path to the key manually.

For example,

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.
```

Value

Field that shows the value of the registry key that is selected in the above tree.

For example, the value for the key

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  
is Shell.
```

Category of protected resources window

In this window, the administrator can select a protected resource.

The following settings are available:

Category of protected resources

Field for entering the name of a category of resources access to which should be protected by Application Privilege Control.

Application Privilege Control adds the created category of protected resources to the current category. You can add both individual protected resources and other categories of protected resources to the newly created category of protected resources.

Select trust group window

In this window, the administrator can select a trust group for applications started before Kaspersky Endpoint Security.

The following settings are available:

Trust groups. A table of trust groups for applications started before Kaspersky Endpoint Security

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups, depending on the level of threat that the applications pose to the operating system.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,

- applications are recorded in the trusted applications database of Kaspersky Security Network,
- the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:

- applications are not digitally signed by trusted vendors,
- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is lower than 50,
- the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:

- applications are not digitally signed by trusted vendors,
- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is in the 51-71 range,
- the user has placed applications in the High Restricted group.



Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:

- applications are not digitally signed by trusted vendors,
- applications are not recorded in the trusted applications database of Kaspersky Security Network,

- the threat index of applications is in the 71-100 range,
- the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.




Inside each trust group, applications are combined into subgroups by vendor name. You can view subgroups by clicking the  icon to the left of the name of a group of applications. You can hide the list of subgroups by clicking the  icon to the left of the name of a group of applications.

The table contains the following columns:

- **Group.** This column shows trust groups and application groups.
- **Network.** This column shows the Firewall response on detecting network activity of an application group that is subject to a set of preset network rules. The Firewall response is designated by an icon that applies to the entire set of pre-configured network rules.

You can change the Firewall action for the entire set of preset network rules in the settings of the Firewall component. If you need to configure Firewall responses for individual network rules, you can do so on the **Network rules** tab of the **Application group control rules** window.

The Firewall action is marked using one of the following icons:

- The  icon signifies that Firewall allows a group of applications to access the network resource.
- The  icon signifies that Firewall blocks a group of applications from accessing the network resource.
- The  icon signifies that you have specified different Firewall responses for a set of preset network rules for an application group on the **Network rules** tab.

If the **Inherit** item has been selected in the context menu of an application group on the **Network rules** tab, the application group inherits the Firewall action from the parent group of applications. The icon is lighter in color than the icons of the parent group of applications.

Device Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Device Control and instructions on how to configure the component settings.

In this section:

About Device Control	319
Device Control subsection.....	320

About Device Control

Device Control ensures the security of confidential data by restricting user access to devices that are installed on the computer or connected to it, including:

- Data storage devices (hard drives, removable drives, tape drives, CD/DVD drives)
- Data transfer tools (modems, external network cards)
- Devices that are designed for converting data to hard copies (printers)
- Connection buses (also referred to as simply "buses"), referring to interfaces for connecting devices to computers (such as USB, FireWire, and Infrared)

Device Control manages user access to devices by applying *device access rules* (also referred to as "access rules") and *connection bus access rules* (also referred to as "bus access rules").

Device Control subsection

In this window, the administrator can perform the following tasks:

- Enable and disable Device Control.
- Form templates for messages about events that occurred during the operation of Device Control.
- Configure rules for user access to computer devices.
- Configure the logging of information about operations with files on removable drives.
- Configure connection bus access rules.
- Create a list of trusted devices.
- Allow or block users from requesting a temporary password to access blocked devices.

The following settings are available:

Enable Device Control

This check box enables / disables the Device Control component.

If the check box is selected, Kaspersky Endpoint Security uses access rules to control access to devices that are connected to the computer.

If the check box is cleared, Kaspersky Endpoint Security does not control access to all devices, so that all users are granted access to all devices that are connected to the computer.

This check box is selected by default.

Device types

The tab displays a table containing all possible types of devices according to the classification of the Device Control component, including their respective access statuses.

The table contains the following columns:

- **Devices.** This column displays the names of the types of devices.

You can sort the list of device access rules by the names of the types of devices. To do this, click the header of the **Devices** column.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of device access rules in reverse alphabetical order. After you click the header of the column for the second time, Kaspersky Endpoint Security sorts the list of device access rules in strict alphabetical order.

- **Access.** This column displays the status of access to the types of devices (*Allow*, *Block*, *Depends on bus*, *Allowed with restrictions*).

A rule is assigned *Allowed with restrictions* status if its status had been *Allowed* and you have changed the rule settings.

Edit

This button opens the **Configuring device access rule** window. You can edit the settings of an access rule in this window.

The button is only available for the access rules for device types which have a file system.

Logging

Clicking this button opens the **Logging Settings** window. This window lets you enable or disable logging of information about operations with files on removable drives. You can also specify an event filter based on file formats or specify users information about whose actions will be logged.

This button is available only for removable drive access rules.

Connection buses

This tab displays a table with a list of all available connection buses according to the Device Control component's classification, including their respective access statuses:

- **Device connection buses.** This column displays the names of the connection buses.

You can sort the list of connection bus access rules by the names of the buses. To do this, click the header of the **Device connection buses** column.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of bus access rules in reverse alphabetical order. After you click the header of the column for the

second time, Kaspersky Endpoint Security sorts the list of bus access rules in strict alphabetical order.

- **Access.** This column displays the statuses of access to the connection buses (*Allow*, *Block*).

Trusted devices

The tab shows a table with the following data:

- **Name.** This column displays the names of the trusted devices.
- **Users.** This column displays the names of the users and / or groups of users who are always granted full access to devices.
- **Comment.** The column shows information about trusted devices that was entered while devices were being added to the Trusted list.
- **Device model / ID.** This column displays the models and / or IDs of trusted devices.
- **Device type.** This column displays the type of a particular device.

You can sort the list of trusted devices by any of the table columns. To do so, left-click the column header.

After you click the header of the column, Kaspersky Endpoint Security sorts the list of trusted devices in reverse alphabetical order. After you click the header of the column for the second time, Kaspersky Endpoint Security sorts the list of trusted devices in strict alphabetical order.

You can change the composition of table columns. To do so, right-click the header of any table column, and in the context menu that opens clear / select check boxes opposite the names of columns that you want to exclude from / include in the table.

You can rearrange the table columns. To do so, left-click a column header and drag it to a new location.

Select

This button opens the **Select trusted devices** window. In this window, you can select one or several devices to add to the list of trusted devices, edit the list of trusted devices, and change the user and/or user group for whom such devices are trusted.

Edit

This button opens the **Configuring device access rule** window for a trusted device. In this window, you can change the user and / or group of users for which the device is specified as trusted.

This button is available if a trusted device is selected from the list of trusted devices.

Delete

This button deletes the selected trusted device from the list of trusted devices.

If the device has been deleted from the list of trusted devices, a decision on access to the device is made based on the access rule that is applied to this device type.

This button is available if a trusted device is selected from the list of trusted devices.

Allow request for temporary access

This check box makes the **Request access** button available / unavailable through the local interface of Kaspersky Endpoint Security.

If the check box is selected, the **Request access** button is available through the local interface of Kaspersky Endpoint Security. Clicking this button opens the **Request access to device** window. In this window, the user can request temporary access to a blocked device.

The check box is only available in the policy properties.

This check box is selected by default.

Templates

This button opens the **Templates** window. In this window, you can edit the template of the message which is displayed when the user attempts to access a blocked device, and the template of the complaint message that is sent to the LAN administrator.

Blockage tab

The entry field contains the template of the message that is displayed when the user attempts to access a blocked device or to perform a forbidden operation with device content.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **Current date (%DATE%).** This variable is replaced with the date when access to the device is blocked or an operation with the device content is forbidden.
- **Current time (%TIME%).** This variable is replaced with the time when access to the device is blocked or an operation with the device content is forbidden.
- **User name (%USER_NAME%).** This variable is replaced with the name of the current user account that has been blocked from an operation with device content.
- **Computer name (%COMPUTER_NAME%).** This variable is replaced with the name of the computer on which access to the device is blocked or an operation with the device content is forbidden.
- **Device type (%DEVICE_TYPE%).** This variable is replaced with the name of the device type to which access is blocked or an operation with the content of which is forbidden.
- **Device name (%DEVICE_NAME%).** This variable is replaced with the name of the device to which access is blocked or an operation with the content of which is forbidden.
- **Operation (%OPERATION%).** This variable is replaced with the name of the type of blocked operation with device content.
- **Device ID (%DEVICE_ID%).** This variable is replaced with the unique identifier of the device to which access is blocked or an operation with the content of which is forbidden.
- **Device model (%DEVICE_VIDPID%).** This variable is replaced with a string that contains the VID and PID of the device to which access is blocked or an operation with the content of which is forbidden.

Link

Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Insert link window

In this window, the administrator can specify the link that will be used in the text of the message template.

The following settings are available:

Web address

Use this field to specify the address of the web resource that opens via the link. This link is added to the text of the message template.

Link text

This field lets you specify the text of the link included in the message. Clicking this text in the message takes you to the web resource whose address is specified in the **Web address** field.

This field is optional. If this field is left blank, the web address of the link is inserted in the message template.

Preview

This field shows the preview of the link in the text of the message template.

Message to administrator tab

The entry field contains a template of the message that is sent to the LAN administrator when the user believes that access to the device is blocked or an operation with device content is forbidden by mistake.

You can edit the text of the template.

To

Field for entering the email address of the LAN administrator.

Subject

Field for entering the subject of the complaint message.

The default subject is `[DeviceControl] Mistaken blocking`.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **Current date (%DATE%).** This variable is replaced with the date when access to the device is blocked or an operation with the device content is forbidden.
- **Current time (%TIME%).** This variable is replaced with the time when access to the device is blocked or an operation with the device content is forbidden.
- **User name (%USER_NAME%).** This variable is replaced with the name of the current user account that has been blocked from an operation with device content.
- **Computer name (%COMPUTER_NAME%).** This variable is replaced with the name of the computer on which access to the device is blocked or an operation with the device content is forbidden.
- **Device type (%DEVICE_TYPE%).** This variable is replaced with the name of the device type to which access is blocked or an operation with the content of which is forbidden.
- **Device name (%DEVICE_NAME%).** This variable is replaced with the name of the device to which access is blocked or an operation with the content of which is forbidden.
- **Operation (%OPERATION%).** This variable is replaced with the name of the type of blocked operation with device content.
- **Device ID (%DEVICE_ID%).** This variable is replaced with the unique identifier of the device to which access is blocked or an operation with the content of which is forbidden.
- **Device model (%DEVICE_VIDPID%).** This variable is replaced with a string that contains the VID and PID of the device to which access is blocked or an operation with the content of which is forbidden.

The method used to send messages and the choice of template depends on whether or not there is an active Kaspersky Security Center policy running on the computer with Kaspersky Endpoint Security installed. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Security Center installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Security Center installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage. The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.
 - If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.
 - If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

Configuring device access rule window

In this window, the administrator can configure the settings of a device access rule.

A device access rule is a combination of parameters that define the following functions of the Device Control component:

- Allowing selected users and / or user group to access specific types of devices during specific periods of time.

You can select a user and / or user group and create a device access schedule for them.

- Setting the right to read the content of memory devices.
- Setting the right to edit the content of memory devices.

By default, access rules are created for all types of devices in the classification of the Device Control component. Such rules grant all users full access to the devices at all times, if access to the connection buses of the respective types of devices is allowed.

To configure access rules, the following settings are available:

Users and / or groups of users

The list contains users and / or groups of users for which the device access rule is configured.

Add

Button which opens the **Select Users or Groups** window in Microsoft Windows. In this window you can select a user and / or group of users for which you want to configure the device access rule.

Edit

Button which opens the **Select Users or Groups** window in Microsoft Windows. In this window, you can change the user and / or group of users for whom you want to configure the device access rule.

This button is available if the entry with the name of the user and / or group of users is selected from the **Users and / or groups of users** list.

Delete

This button deletes the user and / or group of users from the settings of the device access rule.

This button is available if the entry with the name of the user and / or group of users is selected from the **Users and / or groups of users** list.

Rights of the selected group of users by access schedules

This table provides information about restrictions on access to devices: list of device access schedules and a corresponding list of operations that the selected user and / or group of users can perform with devices.

The table contains the following columns:

- **Access schedule.** This column displays the name of a device access schedule. This check box enables / disables the use of a device access schedule for users and / or groups of users that are selected from the **Users and / or groups of users** list.

For a single item on the **Users and / or groups of users** list, you can select multiple device access schedules.

- **Read.** This column shows a check box that determines the right to read the content of devices for the time intervals that are specified in the access schedule when device access is granted:
 - If you want to allow users to view the content of the devices with access controlled by the access rule that you are configuring, select the check box next to the required device access schedule in the **Read** column.
 - If you want to prohibit users to view the content of the devices with access controlled by the access rule that you are configuring, clear the check box next to the required device access schedule in the **Read** column.
- **Write.** This column shows a check box that determines the right to write the content of devices for the time intervals that are specified in the access schedule when device access is granted:
 - If you want to allow users to change the content of the devices to which access is controlled by the access rule that you are configuring, select the check box next to the required device access schedule in the **Write** column.
 - If you want to forbid users to change the content of the devices to which access is controlled by the access rule that you are configuring, clear the check box next to the required device access schedule in the **Write** column.

Create

This button opens the **Schedule for access to devices** window. In this window, you can configure the schedule for device access on specified days of the week. The device access schedule is

applied to users and / or groups of users that are selected in the **Users and / or groups of users** list.

Edit

This button opens the **Schedule for access to devices** window. In this window, you can edit a device access schedule for users and / or groups of users that are selected in the **Users and / or groups of users** list.

The button is available if a device access schedule, other than the default one, is selected from the **Rights of the selected group of users by access schedules** table.

Copy

This button copies the device access schedule that is selected from the **Rights of the selected group of users by access schedules** table.

The button is available if a device access schedule is selected from the **Rights of the selected group of users by access schedules** table.

Delete

This button deletes the selected device access schedule from the table.

The button is available if a device access schedule, other than the default one, is selected from the **Rights of the selected group of users by access schedules** table.

Schedule for access to devices window

In this window, you can configure the schedule for device access on specified days of the week. To do so, specify one or several time periods during which access to devices is monitored, for each day of the week.

Name

Field for entering the name of a device access schedule.

Schedule for access to devices

A device access schedule can be configured by using a special table. Table lines designate days of the week; table columns designate one-hour intervals in the time scale. Depending on the regional settings of the operating system, the time scale may be 24-hour or 12-hour.

The colors of table cells reflect the restrictions that are imposed:

- The gray color signifies that access to devices is not controlled by the device access rule.
- The green color signifies that access to the devices is controlled by the device access rule.

To add a time period to the device access schedule during which access to the device is not monitored, click the cells in the table that correspond to the relevant time and day of the week. The color of the cells turns gray.

To change the time period in the device access schedule during which access to the device is not monitored to a time period during which access to the device is monitored, click the gray cells in the table that correspond to the relevant time and day of the week. The color of the cells turns green.

Logging Settings window

In this window, the administrator can configure the settings for logging events associated with files on removable drives.

The following settings are available:

Enable logging

This check box enables / disables logging of information about operations with files on removable drives.

If the check box is selected, Kaspersky Endpoint Security logs information about write and removal operations performed with files on removable drives and sends a notification to the Kaspersky Security Center Administration Server.

If the check box is cleared, information about operations performed with files on removable drives is not logged anywhere.

This check box is cleared by default.

Write

This check box enables / disables logging of information about write to file operations on removable drives.

If the check box is selected, Kaspersky Endpoint Security logs information about write to file operations on removable drives and sends a notification to the Kaspersky Security Center Administration Server.

If the check box is cleared, information about write to file operations on removable drives is not saved anywhere.

This check box is selected by default.

The check box is available if the **Enable logging** check box is selected.

Delete

This check box enables / disables logging of information about file deletion on removable drives.

If the check box is selected, Kaspersky Endpoint Security logs information about file deletion on removable drives and sends a notification to the Kaspersky Security Center Administration Server.

If the check box is cleared, information about file deletion on removable drives is not saved anywhere.

This check box is cleared by default.

The check box is available if the **Enable logging** check box is selected.

Save information about all files

This check box enables / disables logging of all events.

If the check box is selected, Kaspersky Endpoint Security logs and sends to the Administration Server information about operations performed with all files on removable drives.

If the check box is cleared, Kaspersky Endpoint Security logs and sends to the Administration Server information about operations with files of those formats next to which a check box is selected in the **Filter on file formats** section.

This check box is cleared by default.

Filter on file formats

A list of file formats in connection with which Kaspersky Endpoint Security generates events to be logged and sent to the Administration Server. Each item in the list is a check box.

If the check box next to a file format is selected, Kaspersky Endpoint Security logs and sends to the Administration Server information about operations performed with files of the specified format.

The list includes the following file formats:

- **Text files**
- **Video files**
- **Audio files**
- **Graphic files**
- **Executable files**
- **Office files**
- **Database files**
- **Archives**

By default, check boxes are selected next to the following formats:

- **Text files**
- **Office files**
- **Database files**
- **Archives**

Items in the list are available when the **Save information about all files** check box is cleared.

Users

An entry field for specifying the names of users and / or groups.

When the users specified in this field write to files located on removable drives or delete files from removable drives, Kaspersky Endpoint Security logs the event and sends a message to the Kaspersky Security Center Administration Server.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. This window lets you select users and/or user groups information about whose actions will be logged by Kaspersky Endpoint Security and sent to the Administration Server.

Trusted Wi-Fi networks window

In this window, the administrator can form a list of trusted Wi-Fi networks.

The following settings are available:

Add

Clicking this button opens the **Trusted Wi-Fi network** window. This window lets you specify the settings of the rule according to which a Wi-Fi network is assigned to the trusted group.

Edit

Clicking this button opens the **Trusted Wi-Fi network** window. This window lets you edit the settings of the rule according to which a Wi-Fi network is assigned to the trusted group.

This button is available when a Wi-Fi network is selected in the table.

Delete

Clicking this button removes the selected Wi-Fi network from the list of trusted Wi-Fi networks.

If a Wi-Fi network has been removed from the list of Wi-Fi networks, the connection to this Wi-Fi network is denied in **Block with exceptions** mode.

This button is available when a Wi-Fi network is selected in the table.

Trusted Wi-Fi networks. This table contains information about trusted Wi-Fi networks. In **Block with exceptions** mode, the connection to Wi-Fi networks appearing in this list is allowed.

The table contains the following columns:

- **Network name.** This column shows the name of the Wi-Fi network. The Wi-Fi network with this name is considered trusted. Users are allowed to connect to this Wi-Fi network in **Block with exceptions** operating mode.

- **Authentication type.** This column shows the type of authentication used when connecting to the Wi-Fi network. Wi-Fi networks that use this type of authentication are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** operating mode.
- **Encryption type.** This column shows the type of encryption used to protect Wi-Fi network traffic. Wi-Fi networks that use this type of encryption are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** operating mode.
- **Comment.** This column shows additional information about the rule according to which a Wi-Fi network is assigned to the trusted group.

Trusted Wi-Fi network window

In this window, the administrator can configure the settings that determine which Wi-Fi networks must be considered trusted.

The following settings are available:

Network name

An entry field in which you can specify the name of the Wi-Fi network. The Wi-Fi network with this name is considered trusted. Users are allowed to connect to this Wi-Fi network in **Block with exceptions** mode.

Authentication type

Items in this drop-down list define the type of authentication upon the connection to a Wi-Fi network. Wi-Fi networks that use the specified type of authentication are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** mode.

The following items are available from the **Authentication type** drop-down list:

- **Any.**

If this item is selected, the type of authentication is not considered when determining whether or not a Wi-Fi network belongs to the trusted group.
- **No authentication.**

If this item is selected, Wi-Fi networks that do not require user authentication upon connection are considered trusted.

- **Specified key.**

If this item is selected, the specified key is used for authentication. The specified key corresponds to a specific "sender - recipient" pair.

- **WPA-Enterprise.**

If this item is selected, an extensible authentication protocol for corporate Wi-Fi networks is used. The user must have a certificate authorizing the user to access the Wi-Fi network. To receive this certificate, the user is verified against the database of registered users.

- **WPA-Personal.**

If this item is selected, an extensible authentication protocol for personal Wi-Fi networks is used. A password is set on a wireless router or access point. This password applies to all users.

- **WPA2-Enterprise.**

If this item is selected, the WPA authentication protocol of the second version for corporate Wi-Fi networks is used.

- **WPA2-Personal.**

If this item is selected, the WPA authentication protocol of the second version for personal Wi-Fi networks is used.

The **Any** item is selected by default.

Encryption type

Items in this drop-down list define the type of encryption used to protect Wi-Fi network traffic. Wi-Fi networks that use the specified type of encryption are considered trusted. Users are allowed to connect to these Wi-Fi networks in **Block with exceptions** Device Control mode.

The following items are available from the **Encryption type** drop-down list:

- **Any.**

If this item is selected, the type of encryption is not considered when determining whether or not a Wi-Fi network belongs to the trusted group.

- **Disconnected.**

If this item is selected, Wi-Fi networks that do not use encryption are considered trusted.

- **WEP.**

If this item is selected, Wi-Fi networks that use the Wired Equivalent Privacy algorithm are considered trusted. WEP is based on a stream cipher that allows using a variable key length.

- **TKIP.**

If this item is selected, the Wi-Fi networks that use the Temporal Key Integrity Protocol are considered trusted. A new key is generated for every packet that is transmitted. Keys are generated automatically and sent by the authentication server.

- **AES.**

If this item is selected, the Wi-Fi networks that use the Advanced Encryption Standard symmetrical block cipher algorithm with keys 128, 192, or 256 bits long are considered trusted. The level of encryption (128, 192, or 256 bits) determines the number of number of transformations applied to the data being encrypted.

The **Any** item is selected by default.

Comment. This entry field lets you specify any additional information about the rule according to which a Wi-Fi network is assigned to the trusted group.

Add trusted devices by ID window

In this window, the administrator can add a device to the trusted list based on its ID.

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

If you have added a device to the list of trusted devices and created an access rule for this type of device which blocks or restricts access, Kaspersky Endpoint Security decides whether or not to grant access to the device based on its presence in the list of trusted devices. Presence in the list of trusted devices has a higher priority than an access rule.

To add a device to the trusted list, the following settings are available:

Device type

This drop-down list lets you select the device type. This device type is then used to filter the list of all devices that have been connected to computers that are subject to the policy.

Name / Model

Field for entering the name or model of the device. This parameter is used to filter the consolidated list of all devices that have been connected to computers managed by the policy.

You can enter any number of characters from the name or model of the device.

Computer (by mask)

Field for entering the mask of a computer name. The contents of this field are used to filter the consolidated list of all devices that were connected to computers managed under the policy and have names that contain the name mask entered.

You may enter any number of characters from the computer name and the following special characters:

- * – Represents a sequence of any zero or more characters.
- ? – Represents any single character.

Update

Clicking this button displays the list of all devices connected to computers managed under the policy, for which unique device IDs are known.

Device type

This column displays the type of device.

Name

This column displays the device name.

Device model / ID

This column shows the unique ID of the device.

Computer

This column shows the name of the computer to which the device is connected.

Comment

Additional information on the device.

Allow to users and / or groups of users

A field that lists users and / or groups of users. Those users and / or groups of users are granted full access (read and write) to the device that is selected from the table above.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window you can select the users and / or groups of users to which you want to grant access to devices.

Add trusted devices by model window

In this window, the administrator can add a device to the trusted list based on its model.

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

If you have added a device to the list of trusted devices and created an access rule for this type of device which blocks or restricts access, Kaspersky Endpoint Security decides whether or not to grant access to the device based on its presence in the list of trusted devices. Presence in the list of trusted devices has a higher priority than an access rule.

To add a device to the trusted list, the following settings are available:

Device type

This drop-down list lets you select the device type. This device type is then used to filter the list of all devices that have been connected to computers that are subject to the policy.

Name / Model

Field for entering the name or model of the device. This parameter is used to filter the consolidated list of all devices that have been connected to computers managed by the policy.

You can enter any number of characters from the name or model of the device.

Computer (by mask)

Field for entering the mask of a computer name. The contents of this field are used to filter the consolidated list of all devices that were connected to computers managed under the policy and have names that contain the name mask entered.

You may enter any number of characters from the computer name and the following special characters:

- * – Represents a sequence of any zero or more characters.
- ? – Represents any single character.

Update

Clicking this button displays the list of all devices connected to computers managed under the policy, for which VID and PID settings are known. The VID and PID settings identify the device model.

Device type

This column displays the type of device.

Name

This column displays the device name.

Device model / ID

This column shows the unique ID of the device.

Computer

This column shows the name of the computer to which the device is connected.

Comment

Additional information on the device.

Allow to users and / or groups of users

A field that lists users and / or groups of users. Those users and / or groups of users are granted full access (read and write) to the device that is selected from the table above.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window you can select the users and / or groups of users to which you want to grant access to devices.

Add trusted devices by ID mask window

In this window, the administrator can add a device to the trusted list based on its ID mask.

Trusted devices are devices to which users that are specified in the trusted device settings have full access at all times.

If you have added a device to the list of trusted devices and created an access rule for this type of device which blocks or restricts access, Kaspersky Endpoint Security decides whether or not to grant access to the device based on its presence in the list of trusted devices. Presence in the list of trusted devices has a higher priority than an access rule.

To add a device to the trusted list, the following settings are available:

Device type

This drop-down list lets you select the device type. This device type is then used to filter the list of all devices that have been connected to computers that are subject to the policy.

Mask

Field for entering the name of the device. This name is used to filter the consolidated list of all devices that have been connected to computers that are subject to the policy.

You can enter any number of characters from the device name.

Update

Clicking this button causes a line with a mask for a device model or ID to be added to the table. After you click **OK** in the **Add trusted devices by ID mask** window, the list of trusted devices is supplemented with a rule stipulating that all devices whose models or IDs match the specified mask are considered to be trusted devices by the application.

Device type

This column displays the type of device.

Name

This column displays the device name.

Device model / ID

This column shows the unique ID of the device.

Comment

Additional information on the device.

Allow to users and / or groups of users

A field that lists users and / or groups of users. Those users and / or groups of users are granted full access (read and write) to the device that is selected from the table above.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window you can select the users and / or groups of users to which you want to grant access to devices.

Device Control tab

In this window, the administrator can generate a key to provide a user with access to a blocked device.

The following settings are available:

Browse

Clicking this button opens the standard **Select request file** window in Microsoft Windows. This window lets you select a file with the .akey extension that contains data for a request to access a device:

- Name of the type of device to which the user requests access
- Name of the device to which the user requests access
- Serial number of the device to which the user requests access
- Name of the computer for which the user requests access to the device
- Name of the user account
- Request date.

Save access key

Clicking this button opens the standard **Save access key** window in Microsoft Windows. In this window, you can enter the name of the file with a device access key and select a folder on the computer for saving the file with the device access key.

Web Control

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Web Control and instructions on how to configure the component settings.

In this section:

About Web Control.....	344
Web Control subsection	360

About Web Control

Web Control allows controlling actions by LAN users, by restricting or blocking access to web resources.

A web resource is an individual web page or several web pages, or a website or several websites that have a common feature.

Web Control provides the following options:

- Saving traffic.

Traffic is controlled by restricting or blocking downloads of multimedia files, or by restricting or blocking access to web resources that are unrelated to users' job responsibilities.

- Delimiting access by content categories of web resources.

To save traffic and reduce potential losses from the misuse of employee time, you can restrict or block access to specific categories of web resources (for example, block access to web resources that belong to the "Internet communication media" category).

- Centralized control of access to web resources.

When using Kaspersky Security Center, personal and group settings of access to web resources are available.

All restrictions and blocks that are applied to access to web resources are implemented as rules of access to web resources.

Web resource content categories

The web resource content categories (hereinafter also referred to as "categories") listed below have been selected to most fully describe the blocks of data hosted by web resources, taking into account their functional and thematic features. The order in which the categories appear in this list does not reflect the relative importance or prevalence of such categories on the Internet. The category names are provisional and used solely for purposes of Kaspersky Lab products and websites. The names do not necessarily reflect the meaning implied by law. One web resource can belong to several categories at once.

Adult content

This category includes the following types of web resources:

- Web resources containing any photo or video materials depicting genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources containing any text materials, including literary or artistic materials, describing genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources devoted to a discussion of the sexual aspect of human relations.

Overlaps the "Internet communication media" category.

- Web resources containing erotic materials, works that provide a realistic portrayal of sexual behavior of humans, or works of art designed to stimulate sexual arousal.

- Web resources of official media outlets and online communities with an established target audience, containing a special section and/or individual articles devoted to the sexual aspect of human relations.
- Web resources devoted to sexual perversions.
- Web resources that advertise and sell items for use in sex and stimulation of sexual arousal, sexual services and intimate dating, including services provided online via erotic video chats, "telephone sex", "sexting" ("virtual sex").

Overlaps the "Electronic commerce" category.

This category does not include web resources with scientific, medical, and scholarly content.

Software, audio, video

This category includes the following subcategories that you can individually select:

- **Audio and video.**

This subcategory includes web resources distributing audio and video materials: movies, recordings of sports broadcasts, recordings of concerts, songs, movie clips, videos, tutorial audio and video recordings, etc.

- **Torrents.**

This subcategory includes websites of torrent trackers intended for sharing files of unlimited size.

- **File sharing.**

This subcategory includes file sharing websites irrespective of the physical location of files being distributed.

Alcohol, tobacco, narcotics

This category includes web resources whose content is directly or indirectly related to alcoholic or alcohol-containing products, tobacco products, and narcotic, psychotropic and/or intoxicating substances.

- Web resources that advertise and sell such substances and paraphernalia for consuming them.

Overlaps the "Electronic commerce" category.

- Web resources with instructions on how to consume or produce narcotic, psychotropic, and/or intoxicating substances.

This category includes web resources addressing scientific and medical topics.

Violence

This category includes web resources containing any photo, video or text materials describing acts of physical or psychological violence directed against human beings, or cruel treatment of animals.

- Web resources depicting or describing scenes of executions, torture, or abuse, as well as tools intended for such practices.

Overlaps the "Weapons, explosives, pyrotechnics" category.

- Web resources depicting or describing scenes of murder, fighting, battery, or rape, scenes in which humans, animals, or imaginary creatures are abused or humiliated.
- Web resources with information inciting acts that jeopardize life and/or health, including self-harm or suicide.
- Web resource with information substantiating or justifying the admissibility of violence and/or cruelty, or inciting violent acts against humans or animals.
- Web resources with particularly realistic portrayals or descriptions of victims and atrocities of war, armed conflicts, and military clashes, accidents, catastrophes, natural disasters, industrial or social cataclysms, or human suffering.
- Browser computer games with scenes of violence and cruelty, including the so-called "shooters", "fightings", "slashers", etc.

Overlaps the "Computer games" category.

Weapons, explosives, pyrotechnics

This category includes web resources with information about weapons, explosives, and pyrotechnical products:

- Websites of weapons, explosives, and pyrotechnical products manufacturers and stores.

Overlaps the "Electronic commerce" category.

- Web resources devoted to the manufacture or use of weapons, explosives, and pyrotechnical products.
- Web resources containing analytical, historical, manufacturing, and encyclopedic materials devoted to weapons, explosives, and pyrotechnical products.

The term "weapons" means appliances, items, and means designed to harm the life or health of humans and animals and/or damage equipment and structures.

Profanity

This category includes web resources where profane language has been detected.

Overlaps the "Adult content" category.

This category also includes web resources with linguistic and philological materials containing profanity as the subject of study.

Gambling, lotteries, sweepstakes

This category includes web resources that offer users to participate financially in gambling, even if such financial participation is not a mandatory condition for access to the website. This category includes web resources offering:

- Gambling in which participants are required to make monetary contributions.

Overlaps the "Computer games" category.

- Sweepstakes that involve betting with money.
- Lotteries that involve purchasing lottery tickets or numbers.
- Information that can trigger the desire to participate in gambling, sweepstakes, and lotteries.

Overlaps the "Electronic commerce" category.

This category includes games that offer free-of-charge participation as a separate mode, as well as web resources that actively advertise web resources falling into this category to users.

Network Communications

This category includes web resources that enable users (whether registered or not) to send personal messages to other users of the relevant web resources or other online services and/or add content (either open to public access or restricted) to the relevant web resources on certain terms. You can individually select the following subcategories:

- **Chats and forums.**

This subcategory includes web resources intended for public discussion of various topics using special web applications, as well as web resources designed to distribute or support instant messaging applications that enable real-time communication.

- **Blogs.**

This subcategory includes blog platforms, which are websites that provide paid or free services for creating and maintaining blogs.

- **Social networks.**

This subcategory includes websites designed for building, displaying, and managing contacts between persons, organizations, and governments, which require registration of a user account as a condition of participation.

- **Dating sites.**

This subcategory includes web resources serving as a variety of social networks providing paid or free services.

Overlaps the "Adult content" and "Electronic commerce" categories.

- **Web-based mail.**

This subcategory includes exclusively login pages of an email service and mailbox pages containing emails and associated data (such as personal contacts). This category does not include other web pages of an Internet service provider that also offers email service.

E-tailers, banks, and payment systems

This category includes web resources designed for any online transactions in non-cash monetary funds using special-purpose web applications. You can individually select the following subcategories:

- **Shops and auctions.**

This subcategory includes online shops and auctions selling any goods, work or services to individuals and/or legal entities, including websites of stores that conduct sales exclusively online and online profiles of physical stores that accept online payments.

- **Banks.**

This subcategory includes specialized web pages of banks with online banking functionality, including wire (electronic) transfers between bank accounts, making bank deposits, performing currency conversion, paying for third-party services, etc.

- **Payment systems.**

This subcategory includes web pages of e-money systems that provide access to the user's personal account.

In technical terms, payment can be effected using both bank cards of any types (plastic or virtual, debit or credit, local or international) and e-money. Web resources can fall into this category regardless of whether or not they have such technical aspects as data transmission over the SSL protocol, the use of 3D Secure authentication, etc.

Job search

This category includes web resources designed to bring together employers and job seekers:

- Websites of recruitment agencies (employment agencies and/or headhunting agencies).
- Websites of employers with descriptions of available job openings and their advantages.
- Independent portals with offers of employment from employers and recruitment agencies.
- Professional social networks that, among all else, make it possible to publish or find information about specialists who are not actively searching for employment.

Overlaps the "Internet communication media" category.

Anonymous access systems

This category includes web resources that act as an intermediary in downloading content of other web resources using special web applications for purposes of:

- Bypassing restrictions imposed by a LAN administrator on access to web addresses or IP addresses;
- Anonymously accessing web resources, including web resources that specifically reject HTTP requests from certain IP addresses or their groups (for example, IP addresses grouped by country of origin).

This category includes both web resources intended exclusively for the above mentioned purposes ("anonymizers") and web resources with technically similar functionality.

Computer games

This category includes web resources devoted to computer games of various genres:

- Websites of computer game developers.
- Web resources devoted to a discussion of computer games.

Overlaps the "Internet communication media" category.

- Web resources providing the technical capability for online participation in gaming, together with other participants or individually, with local installation of applications or without such installation ("browser games").
- Web resources designed to advertise, distribute, and support gaming software.

Overlaps the "Electronic commerce" category.

Religions, religious associations

This category includes web resources with materials on public movements, associations, and organizations with a religious ideology and/or cult in any manifestations.

- Websites of official religious organizations at different levels, from international religions to local religious communities.

- Websites of unregistered religious associations and societies that historically emerged by splintering from a dominant religious association or community.
- Websites of religious associations and communities that have emerged independently of traditional religious movements, including at the initiative of a specific founder.
- Websites of inter-confessional organizations pursuing cooperation among representatives of different traditional religions.
- Web resources with scholarly, historical, and encyclopedic materials on the subject of religions.
- Web resources with detailed portrayals or descriptions of the worship as part of religious cults, including rites and rituals involving the worship of God, beings and/or items believed to have supernatural powers.

News media

This category includes web resources with public news content created by the mass media or online publications that let users add their own news reports:

- Websites of official media outlets.
- Websites offering information services with the attribution of official sources of information.
- Websites offering aggregation services, of collections of news information from various official and unofficial sources.
- Websites where news content is created by users themselves ("social news sites").

Overlaps the "Internet communication media" category.

Banners

This category includes web resources with banners. Advertising information on banners may distract users from their activities, while banner downloads increase the amount of traffic.

The web resource content categories (hereinafter also referred to as "categories") listed below have been selected to most fully describe the blocks of data hosted by web resources, taking into account their functional and thematic features. The order in which the categories appear in this list does not reflect the relative importance or prevalence of such categories on the Internet. The category names are provisional and used solely for purposes of Kaspersky Lab products and

websites. The names do not necessarily reflect the meaning implied by law. One web resource can belong to several categories at once.

Adult content

This category includes the following types of web resources:

- Web resources containing any photo or video materials depicting genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources containing any text materials, including literary or artistic materials, describing genitals of humans or humanoid creatures, acts of sexual intercourse or self-stimulation performed by human beings or humanoid creatures.
- Web resources devoted to a discussion of the sexual aspect of human relations.

Overlaps the "Internet communication media" category.

- Web resources containing erotic materials, works that provide a realistic portrayal of sexual behavior of humans, or works of art designed to stimulate sexual arousal.
- Web resources of official media outlets and online communities with an established target audience, containing a special section and/or individual articles devoted to the sexual aspect of human relations.
- Web resources devoted to sexual perversions.
- Web resources that advertise and sell items for use in sex and stimulation of sexual arousal, sexual services and intimate dating, including services provided online via erotic video chats, "telephone sex", "sexting" ("virtual sex").

Overlaps the "Electronic commerce" category.

This category does not include web resources with scientific, medical, and scholarly content.

Software, audio, video

This category includes the following subcategories that you can individually select:

- **Audio and video.**

This subcategory includes web resources distributing audio and video materials: movies, recordings of sports broadcasts, recordings of concerts, songs, movie clips, videos, tutorial audio and video recordings, etc.

- **Torrents.**

This subcategory includes websites of torrent trackers intended for sharing files of unlimited size.

- **File sharing.**

This subcategory includes file sharing websites irrespective of the physical location of files being distributed.

Alcohol, tobacco, narcotics

This category includes web resources whose content is directly or indirectly related to alcoholic or alcohol-containing products, tobacco products, and narcotic, psychotropic and/or intoxicating substances.

- Web resources that advertise and sell such substances and paraphernalia for consuming them.

Overlaps the "Electronic commerce" category.

- Web resources with instructions on how to consume or produce narcotic, psychotropic, and/or intoxicating substances.

This category includes web resources addressing scientific and medical topics.

Violence

This category includes web resources containing any photo, video or text materials describing acts of physical or psychological violence directed against human beings, or cruel treatment of animals.

- Web resources depicting or describing scenes of executions, torture, or abuse, as well as tools intended for such practices.

Overlaps the "Weapons, explosives, pyrotechnics" category.

- Web resources depicting or describing scenes of murder, fighting, battery, or rape, scenes in which humans, animals, or imaginary creatures are abused or humiliated.

- Web resources with information inciting acts that jeopardize life and/or health, including self-harm or suicide.
- Web resource with information substantiating or justifying the admissibility of violence and/or cruelty, or inciting violent acts against humans or animals.
- Web resources with particularly realistic portrayals or descriptions of victims and atrocities of war, armed conflicts, and military clashes, accidents, catastrophes, natural disasters, industrial or social cataclysms, or human suffering.
- Browser computer games with scenes of violence and cruelty, including the so-called "shooters", "fightings", "slashers", etc.

Overlaps the "Computer games" category.

Weapons, explosives, pyrotechnics

This category includes web resources with information about weapons, explosives, and pyrotechnical products:

- Websites of weapons, explosives, and pyrotechnical products manufacturers and stores.

Overlaps the "Electronic commerce" category.

- Web resources devoted to the manufacture or use of weapons, explosives, and pyrotechnical products.
- Web resources containing analytical, historical, manufacturing, and encyclopedic materials devoted to weapons, explosives, and pyrotechnical products.

The term "weapons" means appliances, items, and means designed to harm the life or health of humans and animals and/or damage equipment and structures.

Profanity

This category includes web resources where profane language has been detected.

Overlaps the "Adult content" category.

This category also includes web resources with linguistic and philological materials containing profanity as the subject of study.

Gambling, lotteries, sweepstakes

This category includes web resources that offer users to participate financially in gambling, even if such financial participation is not a mandatory condition for access to the website. This category includes web resources offering:

- Gambling in which participants are required to make monetary contributions.

Overlaps the "Computer games" category.

- Sweepstakes that involve betting with money.
- Lotteries that involve purchasing lottery tickets or numbers.
- Information that can trigger the desire to participate in gambling, sweepstakes, and lotteries.

Overlaps the "Electronic commerce" category.

This category includes games that offer free-of-charge participation as a separate mode, as well as web resources that actively advertise web resources falling into this category to users.

Network Communications

This category includes web resources that enable users (whether registered or not) to send personal messages to other users of the relevant web resources or other online services and/or add content (either open to public access or restricted) to the relevant web resources on certain terms. You can individually select the following subcategories:

- **Chats and forums.**

This subcategory includes web resources intended for public discussion of various topics using special web applications, as well as web resources designed to distribute or support instant messaging applications that enable real-time communication.

- **Blogs.**

This subcategory includes blog platforms, which are websites that provide paid or free services for creating and maintaining blogs.

- **Social networks.**

This subcategory includes websites designed for building, displaying, and managing contacts between persons, organizations, and governments, which require registration of a user account as a condition of participation.

- **Dating sites.**

This subcategory includes web resources serving as a variety of social networks providing paid or free services.

Overlaps the "Adult content" and "Electronic commerce" categories.

- **Web-based mail.**

This subcategory includes exclusively login pages of an email service and mailbox pages containing emails and associated data (such as personal contacts). This category does not include other web pages of an Internet service provider that also offers email service.

E-tailers, banks, and payment systems

This category includes web resources designed for any online transactions in non-cash monetary funds using special-purpose web applications. You can individually select the following subcategories:

- **Shops and auctions.**

This subcategory includes online shops and auctions selling any goods, work or services to individuals and/or legal entities, including websites of stores that conduct sales exclusively online and online profiles of physical stores that accept online payments.

- **Banks.**

This subcategory includes specialized web pages of banks with online banking functionality, including wire (electronic) transfers between bank accounts, making bank deposits, performing currency conversion, paying for third-party services, etc.

- **Payment systems.**

This subcategory includes web pages of e-money systems that provide access to the user's personal account.

In technical terms, payment can be effected using both bank cards of any types (plastic or virtual, debit or credit, local or international) and e-money. Web resources can fall into this category regardless of whether or not they have such technical aspects as data transmission over the SSL protocol, the use of 3D Secure authentication, etc.

Job search

This category includes web resources designed to bring together employers and job seekers:

- Websites of recruitment agencies (employment agencies and/or headhunting agencies).
- Websites of employers with descriptions of available job openings and their advantages.
- Independent portals with offers of employment from employers and recruitment agencies.
- Professional social networks that, among all else, make it possible to publish or find information about specialists who are not actively searching for employment.

Overlaps the "Internet communication media" category.

Anonymous access systems

This category includes web resources that act as an intermediary in downloading content of other web resources using special web applications for purposes of:

- Bypassing restrictions imposed by a LAN administrator on access to web addresses or IP addresses;
- Anonymously accessing web resources, including web resources that specifically reject HTTP requests from certain IP addresses or their groups (for example, IP addresses grouped by country of origin).

This category includes both web resources intended exclusively for the above mentioned purposes ("anonymizers") and web resources with technically similar functionality.

Computer games

This category includes web resources devoted to computer games of various genres:

- Websites of computer game developers.
- Web resources devoted to a discussion of computer games.

Overlaps the "Internet communication media" category.

- Web resources providing the technical capability for online participation in gaming, together with other participants or individually, with local installation of applications or without such installation ("browser games").
- Web resources designed to advertise, distribute, and support gaming software.

Overlaps the "Electronic commerce" category.

Religions, religious associations

This category includes web resources with materials on public movements, associations, and organizations with a religious ideology and/or cult in any manifestations.

- Websites of official religious organizations at different levels, from international religions to local religious communities.
- Websites of unregistered religious associations and societies that historically emerged by splintering from a dominant religious association or community.
- Websites of religious associations and communities that have emerged independently of traditional religious movements, including at the initiative of a specific founder.
- Websites of inter-confessional organizations pursuing cooperation among representatives of different traditional religions.
- Web resources with scholarly, historical, and encyclopedic materials on the subject of religions.
- Web resources with detailed portrayals or descriptions of the worship as part of religious cults, including rites and rituals involving the worship of God, beings and/or items believed to have supernatural powers.

News media

This category includes web resources with public news content created by the mass media or online publications that let users add their own news reports:

- Websites of official media outlets.

- Websites offering information services with the attribution of official sources of information.
- Websites offering aggregation services, of collections of news information from various official and unofficial sources.
- Websites where news content is created by users themselves ("social news sites").

Overlaps the "Internet communication media" category.

Banners

This category includes web resources with banners. Advertising information on banners may distract users from their activities, while banner downloads increase the amount of traffic.

Web Control subsection

In this window, the administrator can perform the following tasks:

- Enable or disable Web Control.
- Use rules to restrict user access to web resources.
- Run diagnostics on created rules of access to web resources.
- Form templates for messages about events that occurred during the operation of Web Control.

The following settings are available:

Enable Web Control

This check box enables / disables the Web Control component.

If the check box is selected, Kaspersky Endpoint Security controls access to websites and their content by all users.

The check box is selected by default.

Add

This button opens the **Rule of access to web resources** window. You can create a new rule in this window.

Edit

This button opens the **Rule of access to web resources** window. You can edit the settings of the selected rule in this window.

This button is available if the rule selected in the list of rules is other than the default rule.

Delete

This button deletes the selected rule.

This button is available if the rule selected in the list of rules is other than the default rule.

Move up

This button moves the selected rule one rank up on the list of rules.

The higher a rule is on the list of rules, the higher priority it has.

Move down

This button moves the selected rule one rank down in the list of rules.

The lower a rule is on the list of rules, the lower priority it has.

Search field

A field for entering a query to search for web resource access rules in the table of access rules sorted by priority. In this field, you can enter the entire contents or any number of characters from the contents of the **Status**, **Rule name**, and **Users** columns.




To view the search results in sequence, use the ◀ and ▶ buttons.

Access rules sorted by priority

A table with web resource access rules.

The table contains the following columns:

- **Status.** This column displays the operating status of the rule:

- *On*. This status means that the rule is used when Web Control is enabled.
- *Off*. This status means that the rule is ignored when Web Control is enabled.
- **Rule name**. This column displays the name of the rule.
- **Users**. This column shows the names of users and / or user groups to which the rule applies.
- **Action**. This column shows the action that is performed by Kaspersky Endpoint Security. Kaspersky Endpoint Security performs this action if the user visits web resources that are described by the web resource access rule:
 - The  icon means that Kaspersky Endpoint Security allows access to web resources that are described by the rule.
 - The  icon means that Kaspersky Endpoint Security blocks access to web resources that are described by the rule.
 - The  icon means that Kaspersky Endpoint Security warns the user that visiting the web resources described by the rule is not recommended.

Diagnostics

This button opens the **Rules diagnostics** window. In this window, you can test web resource access rules.

Templates

This button opens the **Templates** window. In this window, you can edit the templates of the messages which are displayed when web resource access rules are triggered.

Rules diagnostics window

In this window, the administrator can run diagnostics on the created rules for user access to web resources.

The following settings are available:

Specify address

This check box includes / excludes testing of access rules for an individual web resource address in / from the rules diagnostics conditions.

If the check box is selected, the field for entering the address of a web resource is available. Note that the only rules that are tested by the diagnostics are rules whose filters include the entered web resource address.

If the check box is cleared, the field for entering the address of a web resource is not available.

This check box is selected by default.

Specify users and / or groups

This check box enables / disables inclusion of the name of a user and / or user group in the testing of web resource access rules.

If the check box is selected, the **Select** button is available. The **Select** button allows you to open the **Select Users or Groups** window in Microsoft Windows and then select a user and / or user group whose names are taken into account when testing the web resource access rules.

If the check box is cleared, the **Select** button is not available and the web resource access rules are tested for all users.

This check box is selected by default.

Filter content

This check box includes / excludes analysis of content categories and / or data type categories when testing web resource access rules.

If this check box is selected, the **By content categories / By types of data / By content categories and types of data** drop-down list is available.

This check box is selected by default.

By content categories / By types of data / By content categories and types of data

This drop-down list allows you to specify the type of web content filtering.

Possible list values:

- **By content categories.** If this option is selected, a list with the names of content categories is available.

You can select the check boxes next to the names of the content categories for which you want to filter web content.

By default, all check boxes on the list of content category names are cleared.

- **By types of data.** If this option is selected, a list with the names of data type categories is available.

You can select the check boxes next to the names of the data type categories for which you want to filter web content.

By default, all check boxes on the list of data type category names are cleared.

- **By content categories and types of data.** If this option is selected, lists with the names of content categories and data type categories are available.

You can select the check boxes next to the names of the content categories and data type categories for which you want to filter web content.

By default, all check boxes are cleared.

Include time of access attempt

This check box determines whether the time and day of the attempt to access the web resources specified in the rule diagnostics conditions are to be included in / excluded from the test of the web resource access rule.

This check box is selected by default.

Test

This button starts the testing of all currently existing web resource access rules.

After you click the **Test** button, a notification of the action that is performed by Kaspersky Endpoint Security (according to the first triggered rule) is displayed to the right of the button, while **The following rules will also be applied (in order of triggering)** table displays the actions that are performed by Kaspersky Endpoint Security according to the rules that are triggered after the first one.

The button is available if diagnostics conditions are specified.

The following rules will also be applied (in order of triggering)

This table displays information about the actions performed by Kaspersky Endpoint Security according to the second and subsequent rules that are triggered during diagnostics.

The table contains the following columns:

- **Rule name.** This column displays the name of the rule that was triggered during rules diagnostics.
- **Action.** This column displays information about the action that is performed by Kaspersky Endpoint Security according to the triggered rule.

Blockage tab

The entry field contains the template of the message that appears if a rule which blocks access to a web resource is triggered.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **User name (%USER_NAME%).** This variable is replaced with the name of the current account on the computer where the block message is displayed.
- **Web resource address (%CANONIC_REQUEST_URL%).** This variable is replaced with the normalized form of the address of the blocked web resource.
- **Rule name (%RULE%).** This variable is replaced with the name of the rule according to which the web resource is blocked.
- **Email for sending a message (%COMPLAIN_EMAIL%).** This variable is replaced with the email address specified in the **To** field of the complaint message template.

- **Name of content category (%CONTENT_CATEGORY_LIST%).** This variable is replaced with the name of the content category to which the blocked web resource belongs.
- **Name of data type category (%TYPE_CATEGORY_LIST%).** This variable is replaced with the name of the data type category to which the blocked web resource belongs.

Link

Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Message to administrator tab

The entry field contains the template of the message to be sent to the LAN administrator if the user considers the block to be a mistake.

You can edit the text of the template.

To

Field for entering the email address of the LAN administrator.

Subject

Field for entering the subject of the message.

The default subject is `[WebControl] Mistaken blocking`.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **User name (%USER_NAME%).** This variable is replaced with the name of the current account on the computer where the block message is displayed.
- **Web resource address (%CANONIC_REQUEST_URL%).** This variable is replaced with the normalized form of the address of the blocked web resource.

- **Rule name (%RULE%).** This variable is replaced with the name of the rule according to which the web resource is blocked.
- **Name of content category (%CONTENT_CATEGORY_LIST%).** This variable is replaced with the name of the content category to which the blocked web resource belongs.
- **Name of data type category (%TYPE_CATEGORY_LIST%).** This variable is replaced with the name of the data type category to which the blocked web resource belongs.

The method used to send messages and the choice of template depends on whether or not there is an active Kaspersky Security Center policy running on the computer with Kaspersky Endpoint Security installed. The following scenarios are possible:

- If a Kaspersky Security Center policy is not running on the computer that has Kaspersky Security Center installed, a user's message is sent to the local area network administrator by email.

The message fields are populated with the values of fields from the template defined in the local interface of Kaspersky Endpoint Security.

- If a Kaspersky Security Center policy is running on the computer that has Kaspersky Security Center installed, the standard message is sent to the Kaspersky Security Center Administration Server.

In this case, user messages are available for viewing in the Kaspersky Security Center event storage. The message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

- If a Kaspersky Security Center out-of-office policy is running on the computer with Kaspersky Endpoint Security installed, the method used to send messages depends on whether or not there is a connection with Kaspersky Security Center.
 - If a connection with Kaspersky Security Center is established, Kaspersky Endpoint Security sends the standard message to the Kaspersky Security Center Administration Server.
 - If a connection with Kaspersky Security Center is absent, a user's message is sent to the local area network administrator by email.

In both cases, the message fields are populated with the values of fields from the template defined in the Kaspersky Security Center policy.

Warning tab

The entry field consists of a template of the message that is displayed if a rule for warning about attempts to access an unwanted web resource is triggered.

You can edit the text of the template.

By default

This button restores the original text of the template.

Variable

This drop-down button allows you to insert a variable into the text of the template.

Available variables:

- **User name (%USER_NAME%).** This variable is replaced with the name of the current account on the computer where the block message is displayed.
- **Web resource address (%CANONIC_REQUEST_URL%).** This variable is replaced with the normalized form of the address of the blocked web resource.
- **Rule name (%RULE%).** This variable is replaced with the name of the rule according to which the web resource is blocked.
- **Email for sending a message (%COMPLAIN_EMAIL%).** The variable is replaced by the email address specified in the **To** field of the template.
- **Name of content category (%CONTENT_CATEGORY_LIST%).** This variable is replaced with the name of the content category to which the blocked web resource belongs.
- **Name of data type category (%TYPE_CATEGORY_LIST%).** This variable is replaced with the name of the data type category to which the blocked web resource belongs.
- **Link to requested web resource (%CONTINUE_PAGE%).** This variable is replaced with a link to the requested web page.

- **Link to web site (%CONTINUE_SITE%).** This variable is replaced with a link to the website on which the requested web page is located.
- **Link for access to domains (%CONTINUE_DOMAIN%).** This variable is replaced with a link to all existing domains on a level that is lower than or equal to the level marked with the * symbol.

For example, if the address of the blocked web page is `http://www.example.com`, the `%CONTINUE_DOMAIN%` variable is replaced with the link `http://*.example.com`. Clicking this link allows access to such web addresses as `http://www.example.com/*`, `http://domain.example.com/*`, `http://domain.domaine.example.com/*`, where the * wildcard replaces any sequence of zero or more characters.

Link

Clicking this button opens the **Insert link** window. This window lets you add the address of the web resource the link to which you want to add to the text of the block notification.

Rule of access to web resources window

In this window, the administrator can create a rule for user access to web resources.

A web resource access rule is a set of filters and actions that Kaspersky Endpoint Security performs when the user visits web resources that are described in the rule during the time span that is indicated in the rule schedule. Filters allow you to precisely specify a pool of web resources to which access is controlled by the Web Control component.

The following filters are available:

- **Filter by content.** Web Control categorizes web resources by content and data type. You can control user access to web resources with content and data types of certain categories. When the users visit web resources that belong to the selected content category and / or data type category, Kaspersky Endpoint Security performs the action that is specified in the rule.
- **Filter by web resource addresses.** You can control user access to all web resource addresses or to individual web resource addresses and / or groups of web resource addresses.

If filtering by content and filtering by web resource addresses are specified, and the specified web resource addresses and / or groups of web resource addresses belong to the selected content categories or data type categories, Kaspersky Endpoint Security does not control access to all web resources in the selected content categories and / or data type categories. Instead, the application controls access only to the specified web resource addresses and / or groups of web resource addresses.

- **Filter by names of users and user groups.** You can specify the names of users and / or groups of users for which access to web resources is controlled according to the rule.

To create rules of access to web resources, the following settings are available:

Name

Field for entering the name of a web resource access rule.

If the name is not specified, the rule cannot be saved.

Filter content

This drop-down list allows you to set the type of filtering for web content which the user attempts to access.

Possible list values:

- **Any content.** If this value is selected, web content is not filtered.

This value is selected by default.

- **By content categories.** If this value is selected, web content is filtered by content categories and a list of content category names is available.

You can select the check boxes next to the names of the content categories for which you want to filter web content.

By default, all check boxes are cleared.

- **By types of data.** If this value is selected, web content is filtered by data type categories and a list of data type category names is available.

You can select the check boxes next to the names of the data type categories for which you want to filter web content.

By default, all check boxes are cleared.

- **By content categories and types of data.** If this value is selected, web content is filtered by content categories and data type categories; a list with the names of categories is also available.

You can select the check boxes next to the names of the content categories and data type categories for which you want to filter web content.

By default, all check boxes are cleared.

Apply to addresses

This drop-down list allows you to set the list of addresses of the web resources that are covered by the rule.

Possible list values:

- **To all addresses.** If this value is selected, the rule is applied to all addresses of web resources which the user attempts to access.

This value is set by default.

- **To individual addresses.** If this value is selected, the rule is applied to the following list of addresses of web resources.





You can edit, export, or import the list of addresses of web resources by using the following buttons:

- **Add.** This drop-down button allows you to add the address of a web resource or a group of addresses of web resources.
- **Edit.** This button allows you to edit the address of a web resource or a group of addresses of web resources.

This button is available if the address of a web resource or a group of addresses of web resources is selected from the list of addresses of web resources.

- **Delete.** This button allows you to delete the address of a web resource or a group of addresses of web resources.

This button is available if the address of a web resource or a group of addresses of web resources is selected from the list of addresses of web resources.

-  This button exports the entire list of addresses of web resources or its individual items into a .txt file.
-  This button imports the list of addresses of web resources from a .txt file.
-  When this button is clicked, the application copies the items that are selected from the list of addresses of web resources to the clipboard.
-  When this button is clicked, the application inserts elements from the clipboard into the list of addresses of web resources.

Specify users and / or groups

This check box enables / disables the inclusion of names of users and / or groups of users in the rule settings.

If the check box is selected, you can specify users and/or user groups whose access to web resources described by the rule is regulated by this rule. If the check box is selected but no user or user group is selected in the table, the rule cannot be saved.

If the check box is cleared, the rule applies to all users.

This check box is cleared by default.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. This window lets you select or modify users and/or user groups whose access to web resources described by the rule is regulated by this rule.

If the **Specify users and / or groups** check box is cleared, the **Select** button is not available, but the rule is valid for all users.

Action

This drop-down list allows you to set the action that Kaspersky Endpoint Security performs if the user attempts to access a web resource that matches the parameters of the rule.

Possible list values:

- **Allow** If this value is selected, Kaspersky Endpoint Security allows access to web resources that match the parameters of the rule.
- **Block** If this value is selected, Kaspersky Endpoint Security blocks access to web resources that match the parameters of the rule.
- **Warn.** If this value is selected, Kaspersky Endpoint Security displays a message to warn that a web resource is unwanted when the user attempts to access web resources that match the parameters of the rule. By using links from the warning message, the user can obtain access to the requested web resource.

Rule schedule

Drop-down list for selecting a rule schedule. By default, the list contains the **Always** item.

Settings

Clicking this button opens the **Rule schedule** window. In this window you can create a new rule schedule. The rule you have created will be added to the **Rule schedule** drop-down list.

Address / Address mask window

In this window, you can enter the address of a web resource or an address mask.

You can enter an address or web resource address mask in normalized or non-normalized form. If you enter an address or address mask in a non-normalized form, you are automatically prompted to normalize the entered web resource address or address mask.

Groups of addresses window

In this window, the administrator can specify a group of addresses to which the access rule should apply.

The following settings are available:

Groups of addresses of web resources

List of web resource address groups.

The check box opposite the name of the group of web resource addresses includes / excludes the group of web resource addresses in / from a web resource access rule.

Including or excluding a group of addresses in / from a web resource access rule expands or shortens the list of addresses of web resources that are covered by the rule. When the user opens a web resource, the rule manages access to this web resource if the address of the resource has been included in the group of addresses. This rule does not manage access to this web resource if the address of this web resource is not included in the group of addresses and does not fall within any of the selected content categories or data type categories.

Add

Button, which opens the **Group of addresses** window. In this window, you can create a new group of addresses of web resources.

Edit

Button, which opens the **Group of addresses** window. You can edit the settings of a group of addresses of web resources in this window.

The button is available if a group of addresses of web resources is selected.

Delete

This button deletes the selected group of addresses of web resources.

The button is available if a group of addresses of web resources is selected.

Rule schedule window

In this window, the administrator can specify a rule schedule. The rule schedule determines the time span during which Kaspersky Endpoint Security monitors access to web resources covered by the rule.

The following settings are available:

Name

A drop-down list that lets you select a rule schedule to edit the schedule or to use it as the basis for a new rule schedule.

Rename

Clicking this button opens the **Rule schedule name** window. This window lets you edit the name of a rule schedule.

Delete

This button deletes the rule schedule that is selected in the **Name** drop-down list.

Schedule of access to web resources

The rule schedule can be configured by using a special table. Table lines designate days of the week; table columns designate one-hour intervals in the time scale. Depending on the regional settings of the operating system, the time scale may be 24-hour or 12-hour.

The table cell colors reflect the time intervals that are included in, or excluded from, the schedule of the web resource access rule:

- Time intervals that are colored green are included in the rule schedule.
- Time intervals that are colored gray are excluded from the rule schedule.

Save as

Clicking this button opens the **Rule schedule name** window. This window lets you enter the name of the rule schedule to be created on the basis of the changes that are made to the rule schedule that is selected in the **Name** drop-down list.

Data Encryption

If Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for Workstations, data encryption functionality is fully available. If Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)), only encryption of hard drives using BitLocker Drive Encryption technology is available.

This section contains information about encryption and decryption of hard drives, removable drives, and files and folders on local computer drives, and provides instructions on how to configure and perform encryption and decryption of data using Kaspersky Endpoint Security and the Kaspersky Endpoint Security administration plug-in.

When there is no access to encrypted data, follow the special instructions on working with encrypted data.

In this section:

About data encryption	376
Common encryption settings section.....	381
About encryption of hard drives.....	389
Encryption of hard drives section	392

About data encryption

Kaspersky Endpoint Security lets you encrypt files and folders that are stored on local and removable drives, or entire removable drives and hard drives. Data encryption minimizes the risk of information leaks that may occur when a portable computer, removable drive or hard drive is lost or stolen, or when data is accessed by unauthorized users or applications.

If the license has expired, the application does not encrypt new data, and old encrypted data remains encrypted and available for use. In this event, encrypting new data requires the program be activated with a new license that permits the use of encryption.

If the license has expired, or the End User License Agreement has been violated, the key, Kaspersky Endpoint Security, or encryption components has been removed, the encrypted status of previously encrypted files is not guaranteed. This is because some applications, such as Microsoft Office Word, create a temporary copy of files during editing. When the original file is saved, the temporary copy replaces the original file. As a result, on a computer that has no or inaccessible encryption functionality, the file remains unencrypted.

Kaspersky Endpoint Security offers the following aspects of data protection:

- **Encrypting files on local computer drives.** You can compile lists of files by extension or group of extensions and lists of folders stored on local computer drives, and create rules for encrypting files that are created by specific applications. After a Kaspersky Security Center policy is applied, Kaspersky Endpoint Security encrypts and decrypts the following files:
 - Files individually added to lists for encryption and decryption.
 - Files stored in folders added to lists for encryption and decryption.
 - files created by separate applications.

View the *Kaspersky Security Center Administrator's Guide* for details on applying the Kaspersky Security Center policy.

- **Encryption of removable drives.** You can specify a default encryption rule, according to which the application applies the same action to all removable drives, or specify encryption rules for individual removable drives.

The default encryption rule has a lower priority than encryption rules created for individual removable drives. Encryption rules created for removable drives of the specified device model have a lower priority than encryption rules created for removable drives with the specified device ID.

To select an encryption rule for files on a removable drive, Kaspersky Endpoint Security checks whether or not the device model and ID are known. The application then performs one of the following operations:

- If only the device model is known, the application uses the encryption rule (if any) created for removable drives of the specific device model.
- If only the device ID is known, the application uses the encryption rule (if any) created for removable drives with the specific device ID.
- If the device model and ID are known, the application applies the encryption rule (if any) created for removable drives with the specific device ID. If no such rule exists, but there is an encryption rule created for removable drives with the specific device model, the application applies this rule. If no encryption rule is specified for the specific device ID nor for the specific device model, the application applies the default encryption rule.
- If neither the device model nor device ID is known, the application uses the default encryption rule.

The application lets you prepare a removable drive for using encrypted data stored on it in portable mode. After enabling portable mode, you can access encrypted files on removable drives connected to a computer without encryption functionality.

The application performs the action specified in the encryption rule when the Kaspersky Security Center policy is applied.

- **Managing rules of application access to encrypted files.** For any application, you can create an encrypted file access rule that blocks access to encrypted files or allows access to encrypted files only as ciphertext, which is a sequence of characters obtained when encryption is applied.
- **Creating encrypted archives.** You can create encrypted archives and protect access to such archives with a password. The contents of encrypted archives can be accessed only by entering the passwords with which you protected access to those archives. Such archives can be securely transmitted over networks or on removable drives.
- **Encryption of hard drives.** You can select an encryption technology: Kaspersky Disk Encryption or BitLocker Drive Encryption (hereinafter also referred to as simply "BitLocker").

BitLocker is a technology that is part of the Windows operating system. If a computer is equipped with a Trusted Platform Module (TPM), BitLocker uses it to store recovery keys that provide access to an encrypted hard drive. When the computer starts, BitLocker requests the hard drive recovery keys from the Trusted Platform Module and unlocks the drive. You can configure the use of a password and/or PIN code for accessing recovery keys.

You can specify the default hard drive encryption rule and create a list of hard drives to be excluded from encryption. Kaspersky Endpoint Security performs encryption of hard drives sector by sector after the Kaspersky Security Center policy is applied. The application encrypts all logical partitions of hard drives simultaneously. View the *Kaspersky Security Center Administrator's Guide* for details on applying the Kaspersky Security Center policy.

After the system hard drives have been encrypted, at the next computer startup the user must complete authentication using the Authentication Agent before the hard drives can be accessed and the operating system is loaded. This requires entering the password of the token or smart card connected to the computer, or the user name and password of the Authentication Agent account created by the local area network administrator using Authentication Agent account management tasks. These accounts are based on Microsoft Windows accounts under which users log into the operating system. You can manage Authentication Agent accounts and use the Single Sign-On (SSO) technology that lets you log into the operating system automatically using the user name and password of the Authentication Agent account.

If you back up a computer and then encrypt the computer data, after which you restore the backup copy of the computer and encrypt the computer data again, Kaspersky Endpoint Security creates duplicates of Authentication Agent accounts. To remove the duplicate accounts, you must use the `klmover` utility with the `dupfix` key. The `klmover` utility is included in the Kaspersky Security Center build. You can read more about its operation in the *Kaspersky Security Center Administrator's Guide*.

When the application version is upgraded to Kaspersky Endpoint Security 10.0 Service Pack 2 for Windows, the list of Authentication Agent accounts is not saved.

Access to encrypted hard drives is possible only from computers on which Kaspersky Endpoint Security is installed with hard drive encryption functionality (see section "Working with encrypted devices when there is no access to them" on page [242](#)). This precaution minimizes the risk of data leaks from an encrypted hard drive when an attempt to access it is made outside of the local area network of the company.

To encrypt hard drives and removable drives, you can use the **Encrypt used disk space only** function. It is recommended you only use this function for new devices that have not been previously used. If you are applying encryption to a device that is already in use, it is recommended you encrypt the entire device. This ensures that all data is protected - even deleted data that might still contain retrievable information.

Before beginning encryption, Kaspersky Endpoint Security obtains the map of file system sectors. The first wave of encryption includes sectors that are occupied by files at the moment when encryption is started. The second wave of encryption includes sectors that were written to after encryption began. After encryption is complete, all sectors containing data are encrypted.

After encryption is complete and a user deletes a file, the sectors that stored the deleted file become available for storing new information at the file system level but remain encrypted. Thus, as new files are written to a new device during the launch of regular encryption with the **Encrypt only used disk space** function turned on on the computer, after some time all of the sectors will be encrypted.

The data needed to decrypt files is provided by the Kaspersky Security Center Administration Server that controlled the computer at the time of encryption. If the computer with encrypted files has found itself under the control of another Administration Server for any reason and the encrypted files had not been accessed a single time, access can be obtained in one of the following ways:

- request access to encrypted objects from the LAN administrator;
- restoring data on encrypted devices using the Restore Utility;
- Restore the configuration of the Kaspersky Security Center Administration Server that controlled the computer at the time of encryption from a backup copy and use this configuration on the Administration Server that now controls the computer with encrypted objects.

The application creates service files during encryption. Around two to three percent of non-fragmented free space on the hard drive is required to store them. If there is not enough non-fragmented free space on the hard drive, encryption will not start until enough space is freed up.

Compatibility between encryption functionality of Kaspersky Endpoint Security and Kaspersky Anti-Virus for UEFI is not supported. Encryption of hard drives of computers on which Kaspersky Anti-Virus for UEFI is installed renders Kaspersky Anti-Virus for UEFI inoperable.

See also:

Obtaining access to encrypted devices through the application interface	257
Restoring data on encrypted devices using the Restore Utility	259

Common encryption settings section

If the "lock" is open, the settings defined in the policy will not be applied on the client computer with Kaspersky Endpoint Security installed.

Safely delete source files after encryption

This check box enables / disables the feature that permanently deletes source files from local drives after the files have been encrypted.

If the check box is selected, Kaspersky Endpoint Security permanently deletes the source versions of encrypted files from local drives.

This check box is cleared by default.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of this setting in policies of a nested level of the hierarchy. All policies for nested administration groups and slave Administration Servers use the same setting value that is defined in the top-level policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of this setting in policies of a nested level of the hierarchy. On each client computer, Kaspersky Endpoint Security applies the setting value that is specified in policies for the nested administration groups or slave Administration Servers. The setting value does not depend on what is specified in the top-level policy.

The "lock" is closed by default.

The **Password settings** section lets you configure passwords for Authentication Agent, Portable File Manager, and encrypted archives.

Settings

Clicking this button opens the **Encryption password settings** window. This window lets you edit the settings that determine the use of passwords for accessing the encryption settings and encrypted data.

The **Templates** section lets you edit the templates of messages sent to the administrator and the help texts that are displayed in the preboot environment.

Templates

This button opens the **Templates** window. This window lets you edit the templates of email messages that are sent by the user and the administrator to request and grant access to encrypted files, respectively.

Help. Clicking this button opens the **Authentication agent help messages** window. This window lets you edit the text of help messages that are displayed in the Authentication Agent.

Help messages must contain no more than 14 lines and no more than 800 characters. Use of hieroglyphs is not supported.

Authentication agent tab

In this window, the administrator can configure the settings of the password required for the user to complete authentication after encryption of the system hard drive.

The following settings are available for this:

Use Single Sign-On (SSO) technology

This check box enables / disables the use of Single Sign-On (SSO) technology. SSO technology makes it possible to use the same account credentials to access encrypted hard drives and to sign in to the operating system.

If the check box is selected, you have to enter the login name and password of an operating system user to access encrypted hard drives and then automatically log into the operating system.

This check box is selected by default.

Minimum password length – N characters

Field for specifying minimum password length in symbols.

The default value of eight symbols is set.

Assess password strength

This check box allows / blocks access to password strength settings.

If the check box is selected, password strength settings can be edited.

This check box is selected by default.

Capitals must be used

This check box enables / disables a password check for upper-case letters.

If the check box is selected, Kaspersky Endpoint Security checks the password for upper-case letters. The password is rejected if it does not contain upper-case letters.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Digits must be used

This check box enables / disables a password check for numbers.

If the check box is selected, Kaspersky Endpoint Security checks the password for numbers. The password is rejected if it does not contain numbers.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Special characters must be used

This check box enables / disables a password check for the following special symbols: () ` ~ !
@ # \$ % ^ & * - + = | \ { } [] : ; " ' < > , . ? /.

If the check box is selected, Kaspersky Endpoint Security checks the password for special symbols. The password is rejected if it does not contain special characters.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Prohibit matching passwords

This check box enables / disables a password check for a match to the last-used password.

If the check box is selected, Kaspersky Endpoint Security checks the password for a match to a previous password. If the passwords match, the new password is rejected.

This check box is cleared by default.

Change password after N days of use

This check box enables / disables the check of password age.

If the check box is selected, Kaspersky Endpoint Security prompts you to change the password after the specified period has elapsed.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared.

The default value is set to 30 days.

Block password after N failed input attempt(s)

This check box enables / disables a limit on the number of unsuccessful password entry attempts.

If the check box is selected, Kaspersky Endpoint Security blocks password input after the specified number of unsuccessful attempts.

To restore the capability to enter a password, a computer restart is required.

If the check box is cleared, the number of attempts is unlimited.

The default value is set to five attempts.

Prompt active user for password

The status of the check box (selected / cleared) is ignored if the password was previously specified by the corporate LAN administrator or by a user of the client computer. When a policy is applied, the application does not prompt the active user for the password, regardless of the status of the check box.

If no password has been previously specified by a user or administrator, the check box enables / disables prompting of the active user to enter the password for subsequent access to encrypted hard drives.

If the check box is selected, Kaspersky Endpoint Security prompts the active user to enter the password that is required for accessing hard drives after their encryption. If the active user rejects the prompt to set the password, access to hard drives will require entering the password generated automatically before application of the Kaspersky Security Center policy and stored on the Kaspersky Security Center Administration Server. To access hard drives after they have been encrypted, the user must request a password from the LAN administrator.

If this check box is cleared, the application does not prompt the active user for a password. Access to hard drives will require entering the password that was generated automatically before applying the Kaspersky Security Center policy and that was stored on the Kaspersky Security Center Administration Server. To access hard drives after they have been encrypted, the user must request a password from the LAN administrator.

This check box is selected by default.

Use the recommended settings

Clicking this button causes the application to apply password settings recommended by Kaspersky Lab.

This button is available if at least one setting has been modified.

Encrypted packages tab

In this window, the administrator can configure the settings of the password required for the user to work with encrypted packages.

The following settings are available:

Minimum password length – N characters

Field for specifying minimum password length in symbols.

The default value of eight symbols is set.

Assess password strength

This check box allows / blocks access to password strength settings.

If the check box is selected, password strength settings can be edited.

This check box is selected by default.

Capitals must be used

This check box enables / disables a password check for upper-case letters.

If the check box is selected, Kaspersky Endpoint Security checks the password for upper-case letters. The password is rejected if it does not contain upper-case letters.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Digits must be used

This check box enables / disables a password check for numbers.

If the check box is selected, Kaspersky Endpoint Security checks the password for numbers. The password is rejected if it does not contain numbers.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Special characters must be used

This check box enables / disables a password check for the following special symbols: () ` ~ !
@ # \$ % ^ & * - + = | \ { } [] : ; " ' < > , . ? /.

If the check box is selected, Kaspersky Endpoint Security checks the password for special symbols. The password is rejected if it does not contain special characters.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Use the recommended settings

Clicking this button causes the application to apply password settings recommended by Kaspersky Lab.

This button is available if at least one setting has been modified.

Portable File Manager tab

In this window, the administrator can configure the settings of the password required for the user to work with encrypted packages on removable drives using Portable File Manager:

The following settings are available:

Minimum password length – N characters

Field for specifying minimum password length in symbols.

The default value of eight symbols is set.

Assess password strength

This check box allows / blocks access to password strength settings.

If the check box is selected, password strength settings can be edited.

This check box is selected by default.

Capitals must be used

This check box enables / disables a password check for upper-case letters.

If the check box is selected, Kaspersky Endpoint Security checks the password for upper-case letters. The password is rejected if it does not contain upper-case letters.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Digits must be used

This check box enables / disables a password check for numbers.

If the check box is selected, Kaspersky Endpoint Security checks the password for numbers. The password is rejected if it does not contain numbers.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Special characters must be used

This check box enables / disables a password check for the following special symbols: () ` ~ ! @ # \$ % ^ & * - + = | \ { } [] : ; " ' < > , . ? /.

If the check box is selected, Kaspersky Endpoint Security checks the password for special symbols. The password is rejected if it does not contain special characters.

The check box is available if the **Assess password strength** check box is selected.

This check box is selected by default.

Prohibit matching passwords

This check box enables / disables a password check for a match to the last-used password.

If the check box is selected, Kaspersky Endpoint Security checks the password for a match to a previous password. If the passwords match, the new password is rejected.

This check box is cleared by default.

Change password after N days of use

This check box enables / disables the check of password age.

If the check box is selected, Kaspersky Endpoint Security prompts you to change the password after the specified period has elapsed.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared.

The default value is set to 30 days.

Use the recommended settings

Clicking this button causes the application to apply password settings recommended by Kaspersky Lab.

This button is available if at least one setting has been modified.

About encryption of hard drives

Before starting hard drive encryption, the application runs a number of checks to determine if the device can be encrypted, which includes checking the system hard drive for compatibility with Authentication Agent and with BitLocker encryption components. To check for compatibility, the computer must be restarted. After the computer has been rebooted, the application performs all the necessary checks automatically. If the compatibility check is successful, then hard drive encryption starts after the operating system has booted up and application has started. If the system hard drive is found to be incompatible with Authentication Agent or with BitLocker encryption components, the computer must be restarted by pressing the Reset hardware button. Kaspersky Endpoint Security logs information about the incompatibility. Based on this information, the application does not start encryption of hard drives at operating system startup. Information about this event is logged in Kaspersky Security Center reports.

If the hardware configuration of the computer has changed, the incompatibility information logged by the application during the previous check should be deleted in order to check the system hard drive for compatibility with Authentication Agent and BitLocker encryption components. To do so, before hard drive encryption type `avp pbatestreset` in the command line. If the operating system fails to load after the system hard drive has been checked for compatibility with Authentication Agent, you must remove the objects and data remaining after test operation of Authentication Agent by using the Restore Utility and then start Kaspersky Endpoint Security and execute the `avp pbatestreset` command again.

After hard drive encryption has started, Kaspersky Endpoint Security encrypts all data that is written to hard drives.

If the user shuts down or restarts the computer during hard drive decryption, Authentication Agent loads before the next startup of the operating system. Kaspersky Endpoint Security resumes

encryption of hard drives after successful authentication in the authentication agent and the operating system startup.

If the operating system switches to hibernation mode while encrypting hard drives, Authentication Agent loads when the operating system switches back from hibernation mode. Kaspersky Endpoint Security resumes encryption of hard drives after successful authentication in the authentication agent and the operating system startup.

If the operating system goes into sleep mode during hard drive encryption, Kaspersky Endpoint Security resumes encryption of hard drives when the operating system comes out of sleep mode without loading Authentication Agent.

User authentication in the Authentication Agent can be performed in two ways:

- Enter the name and password of the Authentication Agent account created by the LAN administrator using Kaspersky Security Center tools.
- Enter the password of a token or smart card connected to the computer.

The authentication agent supports keyboard layouts for the following languages:

- English (UK)
- English (USA)
- Arabic (Algeria, Morocco, Tunis; AZERTY layout)
- Spanish (Latin America)
- Italian
- German (Germany and Austria)
- German (Switzerland)
- Portuguese (Brazil, ABNT2 layout)
- Russian (for 105-key IBM / Windows keyboards with the QWERTY layout)
- Turkish (QWERTY layout)
- French (France)

- French (Switzerland)
- French (Belgium, AZERTY layout)
- Japanese (for 106-key keyboards with the QWERTY layout)

A keyboard layout becomes available in the Authentication Agent if this layout has been added in the language and regional standards settings of the operating system and has become available on the welcome screen of Microsoft Windows.

If the Authentication Agent account name contains symbols that cannot be entered using keyboard layouts available in the Authentication Agent, encrypted hard drives can be accessed only after they are restored using the Restore Utility (see section "Restoring data on encrypted devices using the Restore Utility" on page [259](#)), or after the Authentication Agent account name and password are restored.

Kaspersky Endpoint Security supports the following tokens, smart card readers, and smart cards:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Smart Card)
- SafeNet eToken 4100 72K Java (Smart Card)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)

- Aladdin-RD JaCarta PKI (USB)
- Aladdin-RD JaCarta PKI (Smart Card)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Reader)
- Gemalto IDPrime .NET 511

Encryption of hard drives section

In this window, the administrator can perform the following tasks:

- Select the encryption technology.
- Select the encryption mode.
- Configure the Authentication Agent settings.
- Enable or disable the **Encrypt used disk space only** function.
- Create a list of exclusions from encryption for **Kaspersky Disk Encryption** technology.
- Configure the settings of the password or PIN code for **BitLocker Drive Encryption** technology.

The following settings are available:

Encryption technology

The items in this drop-down list define the technology that is used for hard drive encryption.

The drop-down list contains the following items:

- **Not specified.** If this item is selected, the application does not perform encryption of hard drives when the Kaspersky Security Center policy is applied.
- **Kaspersky Disk Encryption.** If this item is selected, the application uses full disk encryption (FDE) technology developed by Kaspersky Lab experts when the Kaspersky Security Center policy is applied.

- **BitLocker Drive Encryption.** If this item is selected, the application uses Microsoft technology to encrypt hard drives when the Kaspersky Security Center policy is applied.

If the "lock" is open, the settings defined in the policy will not be applied on the client computer with Kaspersky Endpoint Security installed.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of this setting in policies of a nested level of the hierarchy. All policies for nested administration groups and slave Administration Servers use the same setting value that is defined in the top-level policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of this setting in policies of a nested level of the hierarchy. On each client computer, Kaspersky Endpoint Security applies the setting value that is specified in policies for the nested administration groups or slave Administration Servers. The setting value does not depend on what is specified in the top-level policy.

The "lock" is closed by default.

When **Kaspersky Disk Encryption** technology is selected, you must configure the following settings.

Encryption mode

The items in this drop-down list define the default action that is performed on hard drives by Kaspersky Endpoint Security.

The drop-down list contains the following items:

- **Encrypt all hard drives.** If this item is selected, the application encrypts all hard drives when the Kaspersky Security Center policy is applied.
- **Decrypt all hard drives.** If this item is selected, the application decrypts all previously encrypted hard drives when the Kaspersky Security Center policy is applied.
- **Leave unchanged.** If this item is selected, the application leaves drives in their previous state when the Kaspersky Security Center policy is applied. If the drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted.

This item is selected by default.

Automatically create Authentication Agent accounts for users

Clicking the link embedded in the word *users* opens the **Authentication Agent account creation settings** window. If the check box is selected, applying the policy causes Kaspersky Endpoint Security to create Authentication Agent accounts with the settings specified in the **Authentication Agent account creation settings** window. The list of Authentication Agent accounts can be viewed in the properties of the *Encryption (account management)* local task.

This check box is selected by default.

Add to list of previously created Authentication Agent accounts

If this check box is selected, applying the policy causes Kaspersky Endpoint Security to create Authentication Agent accounts with the settings specified in the **Authentication Agent account creation settings** window that were not previously created. The list of Authentication Agent accounts can be viewed in the properties of the *Encryption (account management)* local task.

This check box is cleared by default.

Save user name entered in Authentication Agent

This check box enables / disables the option that saves the name of the Authentication Agent account that was used for the previous successful authentication.

If the check box is selected, the application saves the name of the Authentication Agent account that was used for the previous successful authentication. You will not be required to enter the account name the next time you attempt to complete authorization in the Authentication Agent under the same account.

If the check box is cleared, the application does not save the name of the Authentication Agent account that was used for the previous successful authentication. You will be prompted to enter the account name the next time you attempt to complete authorization in the Authentication Agent under the same account.

This check box is selected by default.

Encrypt used disk space only

This check box enables / disables the encryption mode in which only occupied sectors of the hard drive are encrypted. This mode is recommended for new drives whose data has not been modified or deleted.

If the check box is selected, only portions of the drive that are occupied by files are encrypted. Kaspersky Endpoint Security automatically encrypts new data as it is added.

If the check box is cleared, the entire drive is encrypted, including residual fragments of previously deleted and modified files.

This check box is cleared by default.

After encryption has been started, enabling / disabling the **Encrypt used disk space only** function will not change this setting. You must select or clear the check box before starting encryption.

Do not encrypt the following hard drives

List of serial numbers belonging to hard drives that were added to exclusions from encryption. Kaspersky Endpoint Security does not encrypt these drives.

Add

Clicking this button opens the **Add devices from Kaspersky Security Center list** window. This window lets you select hard drives that the application should not encrypt.


Delete

Clicking this button deletes the encryption rule for the device that is selected in the table.

This button is available when an entry is selected in the table.

Search field

You can enter any sequence of characters in the search field. A search begins after every change made in the search field.

To reset the search results, delete the contents of the search field or click the  button in the search field.

When **BitLocker Drive Encryption** technology is selected, you must configure the following settings.

Encryption mode

The items in this drop-down list define the default action that is performed on hard drives by Kaspersky Endpoint Security.

The drop-down list contains the following items:

- **Encrypt all hard drives.** If this item is selected, the application encrypts all hard drives when the Kaspersky Security Center policy is applied.
- **Decrypt all hard drives.** If this item is selected, the application decrypts all previously encrypted hard drives when the Kaspersky Security Center policy is applied.
- **Leave unchanged.** If this item is selected, the application leaves drives in their previous state when the Kaspersky Security Center policy is applied. If the drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted.

This item is selected by default.

Allow use of authentication requiring preboot keyboard input on tablets

This check box enables / disables the use of authentication requiring data input in a preboot environment, even if the platform does not have the capability for preboot input (for example, with touchscreen keyboards on tablets).

If the check box is selected, use of authentication requiring preboot input is allowed. It is recommended to use this setting only for devices that have alternative data input tools in a preboot environment, such as a USB keyboard in addition to touchscreen keyboards.

If the check box is cleared, use of authentication requiring preboot input is blocked.

This check box is cleared by default.

Use of hardware encryption

This check box enables / disables use of hardware-based encryption of hard drives.

If the check box is selected, the application applies hardware encryption. This lets you increase the speed of encryption and use less computer resources.

If the check box is cleared, the application uses software encryption.

This check box is selected by default.

Encrypt used disk space only

This check box enables / disables the encryption mode in which only occupied sectors of the hard drive are encrypted. This mode is recommended for new drives whose data has not been modified or deleted.

If the check box is selected, only portions of the drive that are occupied by files are encrypted. Kaspersky Endpoint Security automatically encrypts new data as it is added.

If the check box is cleared, the entire drive is encrypted, including residual fragments of previously deleted and modified files.

This check box is cleared by default.

After encryption has been started, enabling / disabling the **Encrypt used disk space only** function will not change this setting. You must select or clear the check box before starting encryption.

Use Trusted Platform Module (TPM)

If this option is selected, BitLocker uses a Trusted Platform Module (TPM).

A device equipped with a Trusted Platform Module can create encryption keys that can be decrypted only with the device. A Trusted Platform Module encrypts encryption keys with its own root storage key. The root storage key is stored within the Trusted Platform Module. This provides an additional level of protection against attempts to hack encryption keys.

This action is selected by default.

Use PIN

This check box enables / disables the use of a PIN code to obtain access to an encryption key that is stored in a Trusted Platform Module (TPM).

If the check box is selected and a user attempts to access an encryption key, the user is prompted for a PIN code.

If the check box is cleared, the user can access the encryption key without being prompted for a PIN code.

This check box is available if the **Use Trusted Platform Module (TPM)** option has been selected.

This check box is selected by default.

Minimum PIN length

Field for entering the minimum length of the PIN code prompted from the user when the user attempts to access an encryption key that is stored in the Trusted Platform Module (TPM). In this field, you must specify the number of digits.

The field is available if the **Use PIN** check box is selected.

The default length is four digits.

Use password if Trusted Platform Module (TPM) is unavailable

This check box enables / disables the use of a password to obtain access to encryption keys when a Trusted Platform Module (TPM) is not available.

If the check box is selected, the user can use a password to obtain access to encryption keys when a Trusted Platform Module (TPM) is not available.

If the check box is cleared, the user cannot obtain access to encryption keys when a TPM is not available.

This check box is available if the **Use Trusted Platform Module (TPM)** option has been selected.

This check box is selected by default.

Use password

If this option is selected, Kaspersky Endpoint Security prompts the user for a password when the user attempts to access an encrypted drive.

This option can be selected when a Trusted Platform Module (TPM) is not being used.

Minimum password length

Field for entering the minimum length of the password prompted from the user when the user attempts to access an encryption key. You must specify the number of characters in this field.

This field is available if the **Use password if Trusted Platform Module (TPM) is unavailable** check box has been selected or if the **Use password** option has been selected.

The default length is eight characters.

Add devices from Kaspersky Security Center list window

In this window, the administrator can select drives that will be added to the list of exclusions from encryption.

The following settings are available:

Name

A field for entering the hard drive name. This name is used to filter the list of all hard drives connected to computers that are subject to the Kaspersky Security Center policy.

You can enter any number of characters from the hard drive name and use the asterisk symbol (*) to replace a random sequence of characters.

Computer

Field for entering the name of a computer. If the name of a computer is entered, the table containing the list of hard drives displays the hard drives connected to this computer.

You can enter any number of characters from the computer name and use the asterisk symbol (*) to replace a random sequence of characters.

Update

Clicking this button applies the specified filters to the list of hard drives connected to computers that are subject to the policy.

Disk type

A drop-down list whose items let you set a filter for showing hard drives in the table depending on whether or not the operating system is installed on them. This attribute is used to filter the list of all hard drives connected to computers that are subject to a policy:

- **Not considered.** If this option is selected, the table shows all hard drives.
- **Bootable.** If this option is selected, the table shows only those hard drives that have the operating system installed on them.
- **Non bootable.** If this option is selected, the table shows only those hard drives that do not have the operating system installed on them.

The **Not considered** option is selected by default.

Kaspersky Disk Encryption

A drop-down list whose items let you set a filter for showing hard drives in the table depending on whether or not the encryption operation is available for them. This attribute is used to filter the list of all hard drives connected to computers that are subject to a policy:

- **Not considered.** If this option is selected, the table shows all hard drives.
- **Available.** If this option is selected, the table shows only those hard drives for which the encryption operation is available.
- **Not available.** If this option is selected, the table shows only those hard drives for which the encryption operation is unavailable.

The **Not considered** option is selected by default.

Select all

Clicking this button selects the check boxes in the **Name** column opposite the names of all hard drives in the table.

Deselect

Clicking this button clears the check boxes in the **Name** column opposite the names of all hard drives in the table.

Devices from the Kaspersky Security Center list. Table that shows the hard drives of devices that were added to the Kaspersky Security Center list.

If the check box in the line containing the hard drive is selected, Kaspersky Endpoint Security adds this drive to the list of exclusions from encryption. The drive will not be encrypted.

If the check box in the line containing the hard drive is cleared, Kaspersky Endpoint Security does not add this drive to the list of exclusions from encryption. The drive will be encrypted or not encrypted based on the encryption rules defined in the Kaspersky Security Center policy.

The table contains the following columns:

- **Name.** This column shows the name of the hard drive.
- **Device model / ID.** This column shows the unique ID of the device.

- **Computer.** This column shows the name of the computer to which the hard drive is connected.
- **Bootable.** This column shows whether or not the hard drive is a boot disk.
- **Kaspersky Disk Encryption.** This column displays information about whether or not Kaspersky Disk Encryption technology is available for the hard drive.

The availability of BitLocker Drive Encryption does not depend on the value specified in this column.

Viewing the encryption status

To view the encryption status of computer data:

- Open the Administration Console of Kaspersky Security Center.
- In the Managed devices folder of the Administration Console tree, open the folder with the name of the administration group to which the relevant computer belongs.
- In the workspace, select the Devices tab.
- The Devices tab in the workspace shows the properties of computers in the selected administration group.
- On the Devices tab in the workspace, slide the scroll bar all the way to the right.

The Encryption status column shows the encryption status of data on computers in the selected administration group. This status is formed based on information about file encryption on local drives of the computer, encryption of computer hard drives, and encryption of removable drives connected to the computer.

Anti-Virus protection

Kaspersky Endpoint Security provides comprehensive computer protection against various types of threats, network and phishing attacks.

Each type of threat is handled by a dedicated component. Components can be enabled or disabled independently of one another, and their settings can be configured.

In addition to the real-time protection that the application components provide, we recommend that you regularly *scan* the computer for viruses and other threats. This helps to rule out the possibility of spreading malware that is undetected by protection components due to a low security level setting or for other reasons.

Anti-virus protection components refer to the following application components:

- **File Anti-Virus.** This component protects the file system of the computer from infection. File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer and on all connected drives. File Anti-Virus intercepts every attempt to access a file and scans the file for viruses and other threats.
- **Mail Anti-Virus.** This component scans incoming and outgoing email messages for viruses and other threats.
- **Web Anti-Virus.** This component scans traffic that arrives on the user's computer via the HTTP and FTP protocols, and checks whether URLs are listed as malicious or phishing web addresses.
- **IM Anti-Virus.** This component scans traffic that arrives on the computer via IM client protocols. The component lets you securely use many IM clients.
- **System Watcher.** This component keeps a record of application activity on the computer and provides this information to other components to ensure more effective protection of the computer.

The following virus scan tasks are provided in Kaspersky Endpoint Security:

- **Full Scan.** Kaspersky Endpoint Security scans the operating system, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.
- **Custom Scan.** Kaspersky Endpoint Security scans the objects that are selected by the user.

- **Critical Areas Scan.** Kaspersky Endpoint Security scans objects that are loaded at operating system startup, RAM, and objects that are targeted by rootkits.

General Protection Settings section

The **General Settings** section lets you configure an application to start when the computer is turned on, and enable or disable Advanced Disinfection technology.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Start Kaspersky Endpoint Security 10.0 for Windows at computer startup

The check box enables / disables the automatic start of Kaspersky Endpoint Security after the operating system loads.

When the check box is selected, Kaspersky Endpoint Security is started after the operating system loads, protecting the computer during the entire session.

When the check box is cleared, Kaspersky Endpoint Security is not started after the operating system loads until the user starts it manually. Computer protection is disabled and user data may be exposed to threats.

This check box is selected by default.

Use advanced disinfection technology

Advanced disinfection technology is available if Kaspersky Endpoint Security is installed on a computer that runs under Microsoft Windows for workstations. Advanced Disinfection technology is unavailable if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This check box enables / disables the function used by Kaspersky Endpoint Security to enable Advanced Disinfection technology for the computer.

When the check box is selected, on detecting malicious activity in the operating system Kaspersky Endpoint Security shows a pop-up message that suggests performing a special advanced disinfection procedure. After the user approves this procedure, Kaspersky Endpoint Security neutralizes and removes the threat from the computer. After completing the advanced disinfection procedure, Kaspersky Endpoint Security restarts the computer. The advanced disinfection technology uses considerable computing resources, which may slow down other applications.

When the check box is cleared, upon detecting malicious activity in the operating system, Kaspersky Endpoint Security performs the disinfection procedure according to the current values of settings. No computer restart is performed after Kaspersky Endpoint Security neutralizes the threat.

This check box is cleared by default.

The **Objects for detection** section lets you select the types of objects that Kaspersky Endpoint Security should monitor while it is running.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Settings

Clicking this button opens the **Threats** window. In this window, you can modify the list of threats that Kaspersky Endpoint Security detects.

Regardless of the settings, Kaspersky Endpoint Security always detects viruses, worms, and Trojans.

The **Scan exclusions and trusted zone** section lets you create a list of objects that Kaspersky Endpoint Security does not monitor while it is running.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Settings

This button opens the **Trusted zone** window. This window lets you create a list of exclusions, which may include a list of exclusion rules and a list of trusted applications.

A *trusted zone* is a list of objects and applications that Kaspersky Endpoint Security does not monitor when active. In other words, the trusted zone is a set of exclusions from the scope of Kaspersky Endpoint Security protection.

You create a trusted zone depending on the features of the objects that you handle and on the applications that are installed on the computer. You may need to compile a list of exclusion rules or a list of trusted applications if, for example, Kaspersky Endpoint Security blocks access to an object or application which you know to be absolutely safe.

The **Monitored ports** section lets you select the network port monitoring mode in which Mail Anti-Virus, Web Anti-Virus, and File Anti-Virus scan incoming and outgoing data streams.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Monitor all network ports

In this network port monitoring mode, the protection components monitor data streams that are transmitted via any open network ports of the computer.

Monitor selected ports only

In this network port monitoring mode, the protection components monitor only user-specified ports.

A list of network ports that are normally used for transmission of email and network traffic is included in the application distribution kit.

This network port monitoring mode is selected by default.

Settings

This button opens the **Network ports** window. This window lets you create a list of monitored network ports and a list of applications for which Kaspersky Endpoint Security monitors all ports.

This button is available when the **Monitor only selected ports** network port monitoring mode is selected.

Objects for detection window

The **Malware** section lets you gain protection against objects that are categorized as Malicious programs.

Viruses, worms

This check box enables protection against viruses and worms.

Regardless of the application settings, Kaspersky Endpoint Security always detects and blocks viruses and worms. They can cause significant harm to the computer.

Protection against them cannot be disabled.

Trojans

This check box enables protection against Trojans.

Regardless of the application settings, Kaspersky Endpoint Security always detects and blocks Trojans. They can cause significant harm to the computer.

Protection against trojans cannot be disabled.

Malicious tools

This check box enables / disables protection against malicious tools.

When the check box is selected, protection against malicious tools is enabled.

This check box is selected by default.

The **Adware, auto-dialers, other programs** section lets you control adware and legal software that may be used by criminals to damage your computer or personal data.

Adware

This check box enables / disables protection against adware.

When the check box is selected, protection against adware is enabled.

This check box is selected by default.

Auto-dialers

This check box enables / disables protection against auto-dialers.

When the check box is selected, protection against auto-dialers is enabled.

This check box is selected by default.

Other

This check box enables / disables protection against legitimate applications that may be exploited by criminals to harm the user's computer or data (such as Internet chat clients, downloaders, monitoring programs, and remote administration applications).

If the check box is selected, protection is enabled.

This check box is cleared by default.

The **Compressed files** section enables protection against objects that are categorized as Packers.

Packed files that may cause harm

This check box enables / disables protection against packers that can be used by criminals to harm the computer or user data.

When the check box is selected, protection is enabled against packers that intruders can use to harm your computer or personal data.

This check box is selected by default.

Multi-packed files

This check box enables / disables protection against files which have been packed three or more times.

When the check box is selected, protection against multi-packed files is enabled.

This check box is selected by default.

Scan exclusions tab

In this window, the administrator can form a list of exclusions from Anti-Virus scan.

The following settings are available:

Scan exclusions

This table contains information about scan exclusions.

You can exclude the following objects from scanning:

- Files of certain formats
- Files that are selected by a mask
- Selected files
- Folders
- Objects according to the classification of Kaspersky Lab's Virus Encyclopedia

The table contains the following columns:

- **File or folder.** This column contains the check box and the path to a file or folder that has been excluded from scanning by Kaspersky Endpoint Security.

If the check box next to the name of an exclusion is selected, Kaspersky Endpoint Security applies this exclusion during the virus scan.

- **Object name.** This column shows the name of an object that has been excluded from scanning by Kaspersky Endpoint Security. Kaspersky Endpoint Security applies this exclusion if a scan for viruses and other threats detects an object with the specified name.
- **Comment.** This column shows information about a scan exclusion. For a scan exclusion that has been added by default, the column displays information about the vendor.

Add

Clicking this button opens the **Exclusion rule** window. You can create a new exclusion rule in this window.

Edit

Clicking this button opens the **Exclusion rule** window. You can edit the settings of the selected exclusion rule in this window.

This button is available when an element is selected in the **Exclusion rules** table.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete the selected exclusion rule from the list of exclusion rules.

This button is available if an item is selected in the exclusions table.

The **Scan exclusion description** section lets you view the description of the selected exclusion.

This section contains information when an item is selected in the **Scan exclusions** table.

Links in the **Scan exclusion description** section let you edit the settings of the selected exclusion.

File or folder

This item shows the full path to a file or folder that has been specified for the exclusion, in the form of a link. Clicking this link opens the **Name of file or folder** window. You can specify a different file or folder in this window.

This item is available if a file or folder has been selected for the exclusion.

Object name

This item shows the object name that has been specified for the exclusion, in the form of a link. Clicking the link opens the **Object name** window. In this window, you can change the full name of an object according to the classification of the Kaspersky Lab Virus Encyclopedia, or the object name by mask.

This item is available if an object name is selected for the exclusion.

Protection components: any / specified

This element lets you restrict an exclusion to one or more components.

If the **any** value is displayed in the form of a link, all Kaspersky Endpoint Security components apply this exclusion during scanning. Clicking this link causes its value to change to **specified**. The **select components** link appears.

If the **specified** value is displayed in the form of a link, the selected Kaspersky Endpoint Security components apply this exclusion during scanning. Clicking this link causes its value to change to **any**.

The list of components is available when components are selected for the exclusion. Clicking the **select components** link opens the **Protection components** window. This window lets you modify the contents of components that are associated with this exclusion.

Import

Clicking this button opens the standard **Open file** window in Microsoft Windows. In this window, you can select a file with the .dat extension to import a list of scan exclusions.

Export

Clicking this button opens the standard **Save as** window in Microsoft Windows. In this window, you can select a folder and specify the name of the .dat file that contains a list of scan exclusions.

Scan exclusion window

In this window, the administrator can specify the settings of an object added to the list of exclusions.

The following settings are available:

File or folder

This check box enables / disables an option that excludes the selected file or folder from the scan for viruses and other threats.

If the check box is selected, Kaspersky Endpoint Security creates an exclusion for the specified file or folder. Kaspersky Endpoint Security skips them during scanning.

The **File or folder** check box is selected by default in every exclusion.

Object name

This check box enables / disables the option that excludes an object from scanning by its name as it appears in the Kaspersky Lab Virus Encyclopedia.

If the check box is selected, Kaspersky Endpoint Security creates an exclusion for objects with the specified name and excludes objects with the specified name from the scan.

If the **File or folder** and **Object name** check boxes are both selected, Kaspersky Endpoint Security creates an exclusion for the specified file or folder which contains an object with the specified name. In this case, the following conditions apply:

- If a file and object name are specified, only the file containing the object with the specified name is excluded from all subsequent scans.

- If a folder and object name are specified, files in the specified folder which contain objects with the specified name are excluded from all subsequent scans.

Comment

A field for entering additional information about the exclusion rule.

The **Scan exclusion description** section contains a description of the exclusion. You can edit the exclusion settings and specify the Kaspersky Endpoint Security components that use this exclusion in their operation.

Links

Links can be used to edit the settings of an exclusion.

File or folder: [select file or folder](#)

Clicking this link opens the **Name of file or folder** window. In this window, you can specify the name of a file or folder to be skipped by Kaspersky Endpoint Security. You can also specify a file name mask.

This link is available when the **File or folder** check box is selected.

Object name: [enter the object name](#)

Clicking this link opens the **Object name** window. This window lets you specify an object name to have the application exclude objects with the specified name from the scan. The value is specified according to the classification of the Kaspersky Lab Virus Encyclopedia. You can also specify an object name by mask.

The link is available when the **Object name** check box is selected.

Protection components: [any](#) / [specified](#)

The **any** link signifies that this exclusion is used by all components of Kaspersky Endpoint Security.

The **specified** link signifies that this exclusion is used only by the selected components of Kaspersky Endpoint Security.

Clicking the **select components** link opens the **Protection components** window. This window lets you select the components that subsequently use this exclusion in their operation. The **select components** link is displayed if the **specified** link is displayed.

The **any** link is displayed by default.

Protection components window

In this window, the administrator can select which protection components will not perform a virus scan of the specified object.

The following settings are available:

Protection components

List of protection components and tasks of Kaspersky Endpoint Security that use the exclusion rule.

If the check box next to the name of a Kaspersky Endpoint Security protection component or task is selected, that component or task uses the exclusion rule.

By default, all check boxes are cleared for all Kaspersky Endpoint Security protection components and tasks.

Object name window

In this window, the administrator can specify the name of an object added to the list of exclusions.

The following settings are available:

Object name

A field for entering the object name or object name mask. The value is specified according to the classification of the Kaspersky Lab Virus Encyclopedia. Clicking the link www.securelist.com/en/descriptions takes you to the website of the Kaspersky Lab Virus Encyclopedia, which contains details of the object.

For example:

- **not-a-virus:RiskWare.RemoteAdmin.Win32.RAdmin21** – Remote Administrator application designed for remote control of computers; Version 2.1. Author — Dmitry

Znosko, project page – www.famatech.com. In some configurations, the application can be exploited stealthily by an intruder.

- **HackTool.Win32.NetSend** is a hacker tool. It is a Windows program (PE EXE file). It was written in Microsoft Visual C++® and has a size of 10,752 bytes. It is packed by UPX. The unpacked file size is approximately 48 KB. This program serves for sending messages to other computers on the Internet or LAN by using the built-in Windows Messenger Service. The program allows the sender's name to be spoofed. The startup settings involve transmitting the details of the target computer, the spoofed name of the sending computer, and the message text.

File or folder name window

In this window, the administrator can select a file or folder added to the list of exclusions from Anti-Virus scan.

The following settings are available:

File or folder name

A field for entering the file or folder name or mask of the file or folder name.

You can also specify the full path to a file or folder manually. Only file name masks with full paths to files can be entered.

For example:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** – All files in the C:\dir\ folder.
- **C:\dir*.exe** – All files with the .exe extension in the C:\dir\ folder.
- **C:\dir*.ex?** – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- **C:\dir\test** – Only the file C:\dir\test.

Browse

This button opens the **Select folder** window. This window lets you select an object in the object tree.

Include subfolders

This check box enables / disables an option whereby a folder is added to the exclusion rule with all subfolders.

When the check box is selected, Kaspersky Endpoint Security does not scan the folder with all of its subfolders.

When the check box is cleared, Kaspersky Endpoint Security does not scan only the specified folder.

This check box is selected by default.

Trusted applications tab

In this window, the administrator can generate a list of trusted applications whose activity will not be monitored by Kaspersky Endpoint Security.

The following settings are available:

Trusted applications

This table lists trusted applications whose activity is not monitored by Kaspersky Endpoint Security during its operation.

The table contains the following columns:

- **Application.** This column displays a check box and the name of a trusted application.

If the check box next to the name of a trusted application is selected, Kaspersky Endpoint Security scans this application in accordance with the list of exclusions.

The svchost.exe process is added by default.

- **Path.** This column shows the full path to the executable file of a trusted application.

Add

This button opens a context menu. The context menu contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window lists applications that are installed on the computer. You can select any application which you do not want Kaspersky Endpoint Security to scan.

- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. The Open window of Microsoft Windows lets you select the executable file of the application which you do not want Kaspersky Endpoint Security to scan.

Edit

Clicking the button opens the **Scan exclusions for application** window. Use this window to modify the list of application activity types that are skipped during scanning.

This button is available when an element is selected in the **Trusted applications** table.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete a trusted application from the list of trusted applications. Kaspersky Endpoint Security then scans this application during its operation.

This button is available when an element is selected in the **Trusted applications** table.

Import

Clicking this button opens the standard **Open file** window in Microsoft Windows. In this window, you can select a file with the .dat extension to import a list of trusted applications.

Export

Clicking this button opens the standard **Save as** window in Microsoft Windows. In this window, you can select a folder to save the .dat file that contains a list of trusted applications for export.

Exclusions for application window

In this window, the administrator can select which actions of an application added to the trusted list should not be monitored by Kaspersky Endpoint Security.

The following settings are available:

Do not scan opened files

This check box enables / disables the exclusion of all files opened by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan the files that the application opens.

Do not monitor application activity

This check box enables / disables the monitoring of file and network activity of an application in the operating system by the Application Privilege Control, System Watcher, and Firewall components.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of the application.

Do not inherit restrictions of the parent process (application)

This check box enables / disables inheritance by the application of application control rules and application network rules that are specified for the parent process (application).

If the check box is selected, Kaspersky Endpoint Security monitors application activity according to the rules that are specified by the system administrator: file activity is monitored according to application control rules, while network activity is monitored according to application network rules.

If the check box is cleared, Kaspersky Endpoint Security monitors application activity according to application control rules and the application network rules that are inherited from the parent process (application).

Do not monitor child application activity

This check box enables / disables the monitoring of file and network activity of any child application of this application.

If the check box is selected, Kaspersky Endpoint Security does not monitor the file and network activity of child applications of this application.

Do not block interaction with the application interface

The check box enables / disables permission for the application to interact with the Kaspersky Endpoint Security interface.

If the check box is selected, the remote access application is allowed to manage Kaspersky Endpoint Security settings through the Kaspersky Endpoint Security interface.

Do not scan network traffic

This check box enables / disables the exclusion of network traffic generated by the given application from virus scanning.

If the check box is selected, Kaspersky Endpoint Security does not scan incoming and outgoing traffic of this application according to the network traffic exclusion settings. You can configure the exclusion settings in the section that is below the **Do not scan network traffic** setting.

In the section below the **Do not scan network traffic** setting, you can edit the settings of network traffic exclusion from virus scanning.

The section is available if the **Do not scan network traffic** check box is selected.

any / specified remote IP addresses

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote IP addresses.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote IP addresses.

Clicking the **specify** link opens the **Remote IP addresses** window. This window lets you specify the list of IP addresses that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

any / specified remote ports

The **any** link indicates that Kaspersky Endpoint Security does not scan all remote ports.

The **specified** link indicates that Kaspersky Endpoint Security does not scan only the selected remote ports.

Clicking the **specify** link opens the **Remote ports** window. This window lets you specify the list of remote ports that are excluded from scanning. The **specify** link is displayed when the **specified** link is shown.

The **any** link is displayed by default.

Trusted system certificate store tab

In this window, the administrator can select a trusted system certificate store to be used by Kaspersky Endpoint Security to generate a list of exclusions from Anti-Virus scan.

The following settings are available:

Use trusted system certificate store

This check box enables / disables the use of the trusted system certificate storage.

If the check box is selected, Kaspersky Endpoint Security excludes from scanning the applications signed with a trusted digital signature. The Application Privilege Control component automatically assigns such applications to the Trusted group.

If the check box is cleared, a virus scan is performed regardless of whether or not the application has a digital signature. The Application Privilege Control component assigns applications to trust groups according to the configured settings.

This check box is cleared by default.

Trusted system certificate store

Items in this drop-down list define which system certificate storage is considered trusted by Kaspersky Endpoint Security.

The default setting is **Enterprise Trust**.

Network ports window

In this window, the administrator can specify the monitored network ports. Kaspersky Endpoint Security will scan the network activity of applications passing through these ports. The administrator can also select individual applications whose network traffic will be scanned when passing through the monitored ports.

The following settings are available:

Network ports

This table contains network ports and protocols that are normally used for transmission of email and network traffic. This list is included in the Kaspersky Endpoint Security package.

If the check box in this row is selected, Kaspersky Endpoint Security monitors network traffic that passes through this network port via any network protocol.

If the check box in this row is cleared, Kaspersky Endpoint Security temporarily excludes the network port from scanning, but does not remove it from the list of network ports.

By default, all check boxes are selected.

The table contains the following columns:

- **Description.** This column shows the name of the network protocol under which network traffic is transferred through the port most often. The number of the port is indicated in the **Port** column.
- **Port.** This column shows the number of the network port.

Add

Clicking this link opens the **Network port** window. This window lets you add a new network port to the list of network ports that are monitored by Kaspersky Endpoint Security.

Edit

Clicking this link opens the **Network port** window. This window lets you change the network port that is monitored by Kaspersky Endpoint Security.

This link is available when an item is selected in the **Network ports** list.

Delete

Clicking this link causes Kaspersky Endpoint Security to delete the selected network port from the list of network ports.

This link is available when an item is selected in the **Network ports** list.

Monitor all ports for specified applications

This check box enables / disables the option whereby all network ports are monitored for applications that are specified in the **Applications** list.

When the check box is selected, Kaspersky Endpoint Security monitors all network ports for applications that request network access. You can specify these applications in the **Applications** list.

This check box is selected by default.

Applications

A table of applications for which Kaspersky Endpoint Security monitors all network ports. For each application, the path to its executable file is specified. The default list of applications for which Kaspersky Endpoint Security monitors all network ports has been created by Kaspersky Lab.

If the check box next to an application is selected, Kaspersky Endpoint Security monitors all network ports of the application.

If the check box next to an application is cleared, Kaspersky Endpoint Security temporarily does not monitor all network ports of the application.

The check boxes are selected for all applications by default.

The table is available if the **Monitor all ports for specified applications** check box is selected.

The table contains the following columns:

- **Application.** This column shows the application name.
- **Path.** This column shows the path to the executable file of the application.

Add

If you use the local interface of Kaspersky Endpoint Security to generate a list of applications whose network activity should be monitored by Firewall via the above-mentioned ports, clicking the **Add** link opens the context menu. The context menu contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window lists applications that are installed on the computer. From the list of applications, you can select any application for which you want Kaspersky Endpoint Security to monitor all network ports.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. This window lets you specify the executable file of an application for which you want Kaspersky Endpoint Security to monitor all network ports.

If you use the Kaspersky Endpoint Security 10.0 for Windows administration plug-in to generate a list of applications whose network activity should be monitored by Firewall via the network ports specified above, clicking the **Add** link opens the **Application** window. In this window, you can specify the path to the executable file and the application name.

Edit

Clicking this link opens the **Application** window. This window lets you edit the settings of an application for which Kaspersky Endpoint Security monitors all network ports.

This link is available if an item is selected from the **Applications** list.

Delete

This link deletes the selected application from the list of applications.

This link is available if an item is selected from the **Applications** list.

The **Information** section contains warnings about changes that are made to the list of network ports and to the list of applications.

Network port window

In this window, the administrator can add a port to the list of ports monitored by the application.

The following settings are available:

Port

A field for entering the number of the monitored network port.

For example, port 1080.

Description

A field for entering the name of the monitored network port.

Application window

In this window, the administrator can add an application to the list of applications whose network activity is scanned when passing through the monitored ports.

The following settings are available:

Path

A field for entering the path to the executable file of an application for which Kaspersky Endpoint Security monitors all network ports.

Name

A field for entering the name of an application for which Kaspersky Endpoint Security monitors all network ports.

Protecting the computer file system. File Anti-Virus

This section contains information about File Anti-Virus and instructions on how to configure the component settings.

In this section:

About File Anti-Virus	424
File Anti-Virus section	424

About File Anti-Virus

File Anti-Virus prevents infection of the computer's file system. By default, File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer and on all drives that are attached to it for the presence of viruses and other threats.

On detecting a threat in a file, Kaspersky Endpoint Security performs the following:

1. Detects the type of object detected in the file (such as a *virus* or *trojan*).
2. Labels the file as *probably infected* if the scan cannot determine whether or not the file is infected. The file may contain a code sequence that is typical of viruses or other malware, or the modified code of a known virus.
3. The application displays a notification about the malicious object detected in the file (if notifications are configured), and processes the file by taking the action specified in the File Anti-Virus settings.

File Anti-Virus section

File Anti-Virus

This check box enables / disables File Anti-Virus.

If the check box is selected, File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer. By default, File Anti-Virus is configured with the settings that are recommended by Kaspersky Lab specialists.

If the check box is cleared, File Anti-Virus is disabled.

This check box is selected by default.

Buttons and

In the **Security level** section, you can select one of the three file security levels that have been created by Kaspersky Lab specialists, or configure file security level settings on your own. When deciding on a file security level, be sure to take working conditions and the current situation into account.

Buttons and

High

When this file security level is selected, File Anti-Virus takes the strictest control of all files that are opened, saved, and started. File Anti-Virus scans all file types on all hard drives, network drives, and removable storage media of the computer. It also scans archives, installation packages, and embedded OLE objects.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists. File Anti-Virus scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer. It also scans embedded OLE objects. File Anti-Virus does not scan archives or installation packages.

The **Recommended** file security level is the default setting.

Low

The settings of this file security level ensure maximum scanning speed. File Anti-Virus scans only files with specified extensions on all hard drives, network drives, and removable storage media of the computer. File Anti-Virus does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

This button opens the **File Anti-Virus** window. In this window, you can configure file security level settings.

By default

This button sets the file security level to **Recommended**.

The **Action on threat detection** section allows you to select the action that File Anti-Virus performs if infected files are detected during scanning.

Before attempting to disinfect or delete an infected file, File Anti-Virus creates a backup copy for subsequent restoration or disinfection. The backup copy of the file is placed in Backup.

Buttons  and 

Select action automatically

Disinfect. Delete if disinfection fails

Disinfect

Delete

Block

General tab

The **File types** section allows you to select the types of files that File Anti-Virus scans.

File Anti-Virus treats files without extensions as executables. File Anti-Virus always scans them, regardless of the file types that are selected for scanning.

All files

If this setting is selected, File Anti-Virus scans all files without exceptions (all formats and extensions).

Files scanned by format

If this setting is selected, File Anti-Virus scans only potentially infectable files. Before scanning a file for malicious code, the internal header of the file is analyzed to determine the format of the file

(for example, .txt, .doc, or .exe). During scanning, the extension of the file is also taken into account.

This is the default setting.

Files scanned by extension

If this setting is selected, File Anti-Virus scans only potentially infectable files. The file format is then determined based on the file's extension.

Icon ⓘ

Clicking the icon opens the Help system section of Kaspersky Endpoint Security. This section describes a list of file extensions that are scanned by File Anti-Virus.

The **Protection scope** section allows you to create the list of objects that are scanned by File Anti-Virus.

Protection scope

Contains objects that are scanned by File Anti-Virus. A scan object may be a hard drive or network drive, folder, file, or file name mask.

By default, File Anti-Virus scans files that are started on any hard drives, network drives, or removable drives. Objects that are in the **Protection scope** list by default cannot be edited or removed.

If the check box next to the name of a scan object is selected, File Anti-Virus scans it.

If the check box next to the name of a scan object is cleared, File Anti-Virus temporarily excludes it from scanning.

Add

Clicking this button opens the **Select scan scope** window. In this window, you can select objects to be scanned.

Edit

Clicking this button opens the **Select scan scope** window. In this window, you can edit the path to an object to scan.

This button is available if a non-default object has been selected from the list of objects to scan.

Delete

This button removes the selected scan object from the **Protection scope** list.

This button is available if a non-default object has been selected from the list of objects to scan.

Select scan scope window

In this window, the administrator can select an object to add to the scan scope of File Anti-Virus.

The following settings are available:

Object

This field displays the path to the object that is selected from the folder tree above. You can specify a hard drive or network drive, folder, file, or file name mask as an object to be scanned.

You can also enter the path to a scan object manually.

File name masks must be entered with full paths to objects. For example:

- **C:\dir*.*** or **C:\dir*** or **C:\dir** – All files in the C:\dir\ folder.
- **C:\dir*.exe** – All files with the .exe extension in the C:\dir\ folder.
- **C:\dir*.ex?** – All files with the ex? extension in the \C:\dir folder, where ? can be replaced with any single character.
- **C:\dir\test** – Only the file C:\dir\test.

Add

This button adds the path to the selected scan object or file name mask to the **Protection scope** list on the **General** tab of the **File Anti-Virus** window.

Include subfolders

This check box enables / disables scanning of folders that are inside the selected folder. If a subfolder contains other child folders, they are scanned as well. Kaspersky Endpoint Security scans subfolders of all levels.

This check box is selected by default.

List of files scanned by extension

If you selected **Files scanned by extension** in the **File types** section, File Anti-Virus or the virus scan task thoroughly analyzes files with certain extensions for the presence of viruses and other malware.

Kaspersky Endpoint Security considers files without an extension as executable ones.
Kaspersky Endpoint Security always scans executable files regardless of the file types that you select for scanning.

The actual format of a file may not match its file name extension.

File Anti-Virus or the virus scan task scans files with the following extensions:

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

eml – Microsoft Outlook Express message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – extension for a saved Microsoft Office Outlook message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file. Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows.

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates,.xlsx for Microsoft Office Excel 2007

workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xlsm for Microsoft Office Excel 2007 templates with macro support, and xlam for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

thmx – a Microsoft Office 2007 theme

Performance tab

The **Scan methods** section contains methods that File Anti-Virus uses when scanning the computer.

Signature Analysis

Signature analysis uses the Kaspersky Endpoint Security database that contains descriptions of known threats and ways to neutralize them. Protection that uses signature analysis provides a minimally acceptable level of security.

Following the recommendations of Kaspersky Lab's experts, this method is always enabled.

Heuristic Analysis

This check box enables / disables Heuristic Analysis during scanning of the computer.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the detail level for Heuristic Analysis. The detail level for Heuristic Analysis sets the balance between the thoroughness of searching for new threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of detail of Heuristic Analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning executable files for malicious code. At this level of detail, the probability of detecting threats is lower than at the **Medium scan** and **Deep scan** levels. Scanning is faster and less resource-intensive.

The **Light scan** detail level is set by default.

- **Medium scan.** While scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.
- **Deep scan.** While scanning files for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **Light scan** and **Medium scan** detail levels of heuristic analysis. At this level of detail, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels. Scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

Scan only new and changed files

This check box enables / disables the mode of scanning only new files and files that have been modified since the previous scan. File Anti-Virus scans both plain and compound files.

If the mode of scanning only new and modified files is enabled, the links for selecting scanning of all or only new files in the **Scan of compound files** section (**all / new**) become unavailable.

This check box is selected by default.

The **Scan of compound files** section contains a list of compound files that File Anti-Virus scans for viruses and malware.

Scan archives

This check box enables / disables scanning of RAR, ARJ, ZIP, CAB, LHA, JAR, and ICE archives.

This check box is cleared by default.

The following scan options are available for archives:

- **All.** File Anti-Virus scans all archives.
- **New.** File Anti-Virus scans only new archives that have appeared after the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables / disables scanning of installation packages.

This check box is cleared by default.

The following scan options are available:

- **All.** File Anti-Virus scans all installation packages.
- **New.** File Anti-Virus scans only new installation packages that have appeared since the last scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Scan Office formats

This check box enables / disables the feature that File Anti-Virus uses during a virus scan to scan Office format files, including embedded OLE objects.

This check box is selected by default.

The following scan options are available:

- **All.** File Anti-Virus scans all Office format files.
- **New.** File Anti-Virus scans only new Office format files that have appeared since the time of the previous scan.

The setting is available if the **Scan only new and changed files** check box is cleared.

Additional

This button opens the **Compound files** window. In this window, you can specify settings for scanning of compound files.

Compound files window

The **Background scan** section allows you to reduce the time that is required to scan large compound files.

Extract compound files in the background

This check box enables / disables the option of reducing the delay when opening large compound files.

If the check box is selected, Kaspersky Endpoint Security unpacks compound files whose size exceeds the value that is specified in the **Minimum file size** field in the background and with a delay after their detection. Such files can be available for use while they are being scanned. Compound files with a size that is less than the value that is specified in the **Minimum file size** field are available for use only after they are unpacked and scanned.

If the check box is cleared, Kaspersky Endpoint Security unpacks all compound files. Compound files are available for use only after they are unpacked and their contents are scanned.

This check box is cleared by default.

Kaspersky Endpoint Security always scans files that are extracted from archives.

Minimum file size

Field for entering the minimum size of compound files that are available for use while being scanned by Kaspersky Endpoint Security. The value is specified in megabytes.

By default, the file size is set to 0 MB.

The **Size limit** section allows you to limit scanning of compound files that are of a specified size.

Do not unpack large compound files

If this check box is selected, Kaspersky Endpoint Security does not scan compound files if their size exceeds the value that is specified in the **Maximum file size** field.

If this check box is cleared, Kaspersky Endpoint Security scans compound files of all sizes.

Kaspersky Endpoint Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is selected.

Maximum file size

Kaspersky Endpoint Security does not unpack files that are larger than the specified value. The value is specified in megabytes.

By default, the file size is set to 8 MB.

Additional tab

The **Scan mode** section allows you to select a condition that triggers file scanning by File Anti-Virus.

Smart mode

In this scan mode, File Anti-Virus scans files by analyzing operations that are performed with a file by the user, an application on behalf of the user (under the currently active account or a different user account), or the operating system.

This mode is used by default.

On access and modification

In this scan mode, File Anti-Virus scans files when the user or an application on behalf of the user (under the currently active account or a different user account) or the operating system attempts to open or modify the files.

On access

In this scan mode, File Anti-Virus scans files only when the user or an application on behalf of the user (under the currently active account or a different user account) or the operating system attempts to open the files.

On execution

In this scan mode, File Anti-Virus scans files only when the user or an application on behalf of the user (under the currently active account or a different user account) or the operating system attempts to launch the files.

The **Scan technologies** section contains scan technologies that File Anti-Virus uses when scanning files. By default, the iChecker and iSwift technologies are mutually complementary. This speeds up anti-virus scanning of objects that are from various file systems and operating systems.

iSwift Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any changes made to the scan settings. The iSwift technology is an improvement on the iChecker technology for the NTFS file system.

The check box enables / disables the use of iSwift technology.

This check box is selected by default.

iChecker Technology

This technology increases scanning speed by excluding certain files from scanning. Files are excluded from scanning by using a special algorithm that takes into account the release date of Kaspersky Endpoint Security databases, the date that the file was last scanned on, and any modifications to the scanning settings.

The check box enables / disables the use of iChecker technology.

This check box is selected by default.

The **Pause task** section allows you to pause File Anti-Virus.

By schedule

The check box enables / disables the option that allows pausing File Anti-Virus for a specified time. This feature can decrease the load on the operating system.

This check box is cleared by default.

Schedule

This button opens the **Pause task** window. In this window, you can specify the time interval for which File Anti-Virus is paused.

The button is available if the **By schedule** check box is selected.

At application startup

This check box enables / disables the option which pauses File Anti-Virus for the time period during which the user works with applications that require significant resources from the operating system.

This check box is cleared by default.

Select

This button opens the **Applications** window. In this window, you can create a list of applications that pause File Anti-Virus when they are running.

The button is available if the **At application startup** check box is cleared.

Pause task window

In this window, the administrator can specify the time to pause and resume File Anti-Virus.

The following settings are available:

Pause task at

Field for entering the time at which File Anti-Virus pauses. The time is specified in HH:MM format.

Resume task at

Field for entering the time at which File Anti-Virus resumes. The time is specified in HH:MM format.

Applications window

In this window, the administrator can form a list of applications that, when started, will cause File Anti-Virus to terminate its operation.

The following settings are available:

Applications

This list includes applications during whose operation Kaspersky Endpoint Security pauses File Anti-Virus. For each application the list includes the path to its corresponding executable file.

Add

This button opens a context menu. The context menu contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window displays a list of applications that are currently running. You can select any application from the list.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. In this window, you can specify the executable application file that you are adding to the list.

Edit

This button opens a context menu. Use context menu items to replace the application that is selected from the list with another one. The context menu of the button contains the following items:

- **Applications.** Use this item to go to the **Select application** window. The **Select application** window displays a list of applications that are currently running. You can select any application from the list.
- **Browse.** Use this item to go to the standard **Open** window of Microsoft Windows. In this window, you can specify the executable application file that you want to use to replace the one from the list in the **Applications** window.

This button is available if an item is selected from the **Applications** list.

Delete

This button removes the selected application from the list.

This button is available if an item is selected from the **Applications** list.

Select application window

In this window, the administrator can add an application that, when started, will cause File Anti-Virus to terminate its operation.

The following settings are available:

Search field

In the search field, you can enter the full name of an application or a keyword from its name to find the application in the **Select application from the list** table. All applications with names that contain the characters that are entered in the search field are displayed in the table under the search field.

To reset the search results, delete the contents of the search field.

Select application from the list

This table displays the applications that are installed on the user's computer.

The table contains the following columns:

- **Application.** This column shows the name of an application that is installed on the user's computer.
- **Vendor.** This column displays the name of the vendor of an application that is installed on the user's computer.
- **File.** This column shows the full path to the executable file of the application.

Email protection. Mail Anti-Virus

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Mail Anti-Virus and instructions on how to configure the component settings.

In this section:

About Mail Anti-Virus.....	441
Mail Anti-Virus section.....	442

About Mail Anti-Virus

Mail Anti-Virus scans incoming and outgoing email messages for viruses and other threats. It starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all messages that are sent or received via the POP3, SMTP, IMAP, MAPI, and NNTP protocols. If no threats are detected in the message, it becomes available and/or is processed.


On detecting a threat in an email message, Mail Anti-Virus performs the following:

1. Identifies the type of object detected in the email message (such as a *trojan*).
2. An email message is assigned one of the following statuses:
 - *Probably infected*. This status is assigned if the scan cannot determine whether or not the email message is definitely infected. The email message may possibly contain a section of code that is typical of viruses or other malware, or the modified code of a known virus.

- *Infected.* This status is assigned to an object if the scan of an email message finds a section of code of a known virus that is included in the anti-virus databases of Kaspersky Endpoint Security.
- *Not found.* This status is assigned to an object if the scan of an email message does not detect viruses or other threats.

The application then blocks the email message, displays a notification about the detected object (if this is specified in the notification settings), and performs the action that is specified in the settings of Mail Anti-Virus.

This component interacts with mail clients installed on the computer. An embeddable extension is available for the Microsoft Office Outlook® mail client that lets you fine-tune the message scan settings. The Mail Anti-Virus extension is embedded in the Microsoft Office Outlook mail client during installation of Kaspersky Endpoint Security.

Operation of Mail Anti-Virus is signified by the application icon displayed in the taskbar notification area. When Mail Anti-Virus is scanning an email message, the application icon changes to .

Mail Anti-Virus section

Mail Anti-Virus

This check box enables / disables Mail Anti-Virus.

When the check box is selected, Mail Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all email messages that are transmitted via the POP3, SMTP, IMAP, MAPI, and NNTP protocols.

When the check box is cleared, Mail Anti-Virus is disabled.

This check box is selected by default.

Buttons and

The **Security level** section allows you to select one of three email security levels that are preconfigured by Kaspersky Lab's experts, or configure a custom email security level on your own. When deciding on an email security level, be sure to take into account the working conditions and current situation.

Buttons and

High

When this email security level is selected, Mail Anti-Virus performs the strictest control of email messages. Mail Anti-Virus scans incoming and outgoing messages, and performs deep heuristic analysis.

The **High** mail security level is recommended when working in a dangerous environment. An example of such an environment is a connection to a free email service from a home network that is not guarded by centralized email protection.

Recommended

The email security level that provides the optimal balance between the performance of Kaspersky Endpoint Security and email security. Mail Anti-Virus scans incoming and outgoing email messages, and performs medium-level heuristic analysis. This mail traffic security level is recommended by Kaspersky Lab specialists.

The **Recommended** mail security level is the default setting.

Low

When this email security level is selected, Mail Anti-Virus only scans incoming email messages, performs light heuristic analysis, and does not scan archives that are attached to email messages. At this mail security level, Mail Anti-Virus scans email messages at maximum speed and uses a minimum of operating system resources.

The **Low** mail security level is recommended for use in a well-protected environment. An example of such an environment might be a LAN with centralized email security.

Custom

Email security level with your custom settings.

Settings

This button opens the **Mail Anti-Virus** window. In this window, you can configure the email security level settings.

By default

This button sets the email security level to **Recommended**.

The **Action on threat detection** section allows you to select the action that Mail Anti-Virus performs if scanning reveals that an email message is infected.

Before attempting to disinfect or delete an infected email message, Mail Anti-Virus creates a backup copy of it so that it can be restored or disinfected later.

Buttons  and 

Select action automatically

Disinfect. Delete if disinfection fails

Disinfect

Delete

Block

General tab

The **Protection scope** section allows you to select the type of email messages that are scanned by Mail Anti-Virus.

Incoming and outgoing messages

If this setting is selected, Mail Anti-Virus scans both incoming and outgoing email messages.

This is the default setting.

Incoming messages only

If this option is selected, Mail Anti-Virus scans only incoming email messages.

The **Connectivity** section lets you configure the scanning of email traffic by Mail Anti-Virus and the settings of Mail Anti-Virus embedding into email clients.

POP3 / SMTP / NNTP / IMAP traffic

The check box enables / disables scanning by Mail Anti-Virus of traffic that is transferred via the POP3, SMTP, NNTP, and IMAP protocols before it arrives on the receiving computer.

If the check box is selected, Mail Anti-Virus scans email messages that arrive via the POP3, SMTP, NNTP, and IMAP protocols before they are received on the computer.

When the check box is cleared, Mail Anti-Virus does not scan email messages that are transferred via the POP3, SMTP, NNTP, and IMAP protocols before they arrive on your computer. In this case, email messages are scanned by the Mail Anti-Virus plug-in that is embedded in Microsoft Office Outlook email client after email messages arrive on the user's computer.

This check box is selected by default.

Additional: Microsoft Office Outlook extension

If the check box is selected, you can configure the Mail Anti-Virus settings from Microsoft Office Outlook and specify when Mail Anti-Virus should scan email messages for viruses. Scanning of email messages transmitted via POP3, SMTP, NNTP, IMAP, and MAPI protocols is enabled on the side of the extension integrated into Microsoft Office Outlook. Scanning is performed after messages have been received on the user's computer.

If the check box is cleared, Mail Anti-Virus settings cannot be configured from Microsoft Office Outlook. Scanning of email messages transmitted via POP3, SMTP, NNTP, IMAP, and MAPI protocols after they have been received on the user's computer is disabled on the side of the extension integrated into Microsoft Office Outlook.

This check box is selected by default.

The **Scan of compound files** section contains the settings for scanning objects attached to email messages.

Scan attached archives

This check box enables / disables the option where Mail Anti-Virus scans archives that are attached to email messages.

This check box is selected by default.

Scan attached Office formats

This check box enables / disables the option where Mail Anti-Virus scans Office format files that are attached to email messages.

This check box is selected by default.

Do not scan archives larger than

The check box enables / disables the option where Mail Anti-Virus scans archives that are attached to email messages depending on the size of the archives. This feature can accelerate scanning of email messages.

The maximum size of archives attached to email messages is specified in megabytes.

By default, the value is set to 8 MB.

If this check box is selected, Mail Anti-Virus excludes archives attached to email messages from scanning if their size exceeds the specified value. A field for specifying the maximum size of archives attached to email messages.

If the check box is cleared, Mail Anti-Virus scans email attachment archives of any size.

This check box is cleared by default.

The check box is available if the **Scan attached archives** check box is selected.

Do not scan archives for more than

The check box enables / disables the option that limits the amount of time that is allocated for scanning archives attached to email messages.

The maximum scan time for archives attached to email messages is specified in seconds.

The default value is 5 seconds.

If the check box is selected, the time that is allocated for scanning archives attached to email messages is limited to the specified period. A field for specifying the maximum time for scanning archives attached to email messages.

This check box is cleared by default.

The check box is available if the **Scan attached archives** check box is selected.

Email protection window

In this window, the administrator can configure the email scan settings using the Mail Anti-Virus extension for Outlook.

The following settings are available:

Scan when receiving

This check box enables / disables the scanning of email messages as they are received.

If the check box is selected, Mail Anti-Virus analyzes each message as it arrives to the mailbox.

If the check box is cleared, Mail Anti-Virus does not scan a message as it is received.

This check box is selected by default.

Scan when reading

This check box enables / disables the scanning of email messages when they are read.

If the check box is selected, Mail Anti-Virus scans a message when the user opens it to read it.

If the check box is cleared, Mail Anti-Virus does not scan a message when it is opened to be read.

This check box is selected by default.

Scan when sending

This check box enables / disables the scanning of email messages as they are sent.

If the check box is selected, Mail Anti-Virus analyzes each outgoing message as it is being sent.

If the check box is cleared, Mail Anti-Virus does not scan outgoing messages as they are being sent.

This check box is selected by default.

If mail is scanned using the Mail Anti-Virus extension for Outlook, it is recommended to use Cached Exchange Mode. For more detailed information about the Exchange caching mode and recommendations on its use, please refer to the Microsoft Knowledge Base:

<https://technet.microsoft.com/en-us/library/cc179175.aspx>.

Attachment filter tab

In this window, the administrator can configure a filter by which Mail Anti-Virus will pick out email message attachments to undergo a virus scan.

The following settings are available:

Disable filtering

If this setting is selected, Mail Anti-Virus does not filter files that are attached to email messages.

This is the default setting.

Rename selected attachment types

If this setting is selected, Mail Anti-Virus replaces the last character in attached files of the specified types with the underscore (_) symbol.

Delete selected attachment types

If this setting is selected, Mail Anti-Virus deletes attached files of the specified types from email messages.

You can specify the types of attached files to delete from email messages in the list of file masks.

File masks

A list of file masks that Mail Anti-Virus either renames or deletes after filtering attachments in email messages.

The list of file masks is available if the **Rename specified attachment types** option or the **Delete specified attachment types** option is enabled.

If the check box next to the file mask is selected, Mail Anti-Virus renames or deletes files of this type when filtering email attachments.

If the check box next to the file mask is cleared, Mail Anti-Virus skips files of this type without any changes when filtering email attachments.

Add

This button opens the **File mask** window. In this window, you can enter a file mask to add to the list of file masks.

Edit

This button opens the **File mask** window. In this window, you can change an existing file mask.

The button is available if an item in the list of file masks is selected.

Delete

This button deletes the selected item from the list of file masks.

The button is available if an item in the list of file masks is selected.

File mask window

In this window, the administrator can specify a mask for files forwarded in email attachments that must be scanned by Mail Anti-Virus.

The following setting is available:

File mask

The field for entering the file mask in accordance with which Mail Anti-Virus filters attachments in email messages.

Additional tab

In this window, the administrator can configure the heuristic analysis settings for Mail Anti-Virus.

The following settings are available:

Heuristic Analysis

This check box enables / disables the use of heuristic analysis during Mail Anti-Virus email scans.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the heuristic analysis level. The heuristic analysis level ensures a balance between the thoroughness of scanning for threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of heuristic analysis are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files while scanning email for malicious code. At this heuristic analysis level, the probability of detecting threats is lower than at the **medium scan** and **deep scan** heuristic analysis levels. Email scanning is faster and less resource-intensive.

- **Medium scan.** When scanning files for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab.

The **medium scan** heuristic analysis level is selected by default.

- **Deep scan.** When scanning mail for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **light scan** and **medium scan** levels of heuristic analysis. At this heuristic analysis level, the probability of detecting threats is higher than at the **Light** and **Medium** levels of heuristic analysis. Email scanning consumes more system resources and takes more time.

The slider is available if the **Heuristic analysis** check box is selected.

Computer protection on the Internet. Web Anti-Virus

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about Web Anti-Virus and instructions on how to configure the component settings.

In this section:

About Web Anti-Virus	451
Web Anti-Virus section	452

About Web Anti-Virus

Every time you go online, you expose information that is stored on your computer to viruses and other malware. They can infiltrate the computer while the user is downloading free software or browsing websites that are compromised by criminals. Network worms can find a way onto your computer as soon as you establish an Internet connection, even before you open a web page or download a file.

Web Anti-Virus protects incoming and outgoing data that is sent to and from the computer over the HTTP and FTP protocols and checks URLs against the list of malicious or phishing web addresses.

Web Anti-Virus intercepts and analyzes for viruses and other threats every web page or file that is accessed by the user or an application via the HTTP or FTP protocol. The following happens next:

- If the page or file is found not to contain malicious code, the user gains immediate access to them.

- If a user accesses a web page or file that contains malicious code, the application performs the action that is specified in the Web Anti-Virus settings.

Web Anti-Virus section

Web Anti-Virus

Buttons  and 

The **Security level** section allows you to select one of three security levels for web traffic that are preconfigured by Kaspersky Lab, or configure your own custom security level. When deciding on the web traffic security level, be sure to take into account the working conditions and current situation.

Buttons  and 

High

The security level under which Web Anti-Virus performs maximum scanning of web traffic that the computer receives via the HTTP and FTP protocols. Web Anti-Virus thoroughly scans all web traffic objects using the full set of application databases, and performs the deepest possible heuristic analysis.

Recommended

The security level that provides the optimal balance between the performance of Kaspersky Endpoint Security and the security of web traffic. Web Anti-Virus performs heuristic analysis at the **medium scan** level. This web traffic security level is recommended by Kaspersky Lab specialists.

The **Recommended** web traffic security level is set by default.

Low

The settings of this web traffic security level ensure the fastest scanning of web traffic. Web Anti-Virus performs heuristic analysis at the **light scan** level.

Custom

Web traffic security level with your custom settings.

Settings

This button opens the **Web Anti-Virus** window. In this window you can configure the security level settings for web traffic.

By default

This button sets the web traffic security level to **Recommended**.

The **Action on threat detection** section allows you to select an action to be performed by Web Anti-Virus if scanning web traffic reveals that an object contains malicious code.

Buttons and

Select action automatically

If this action is selected, on detection of an infected object in web traffic Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. The default action is **Block download**.

Block download

If this action is selected, on detection of an infected object Web Anti-Virus blocks access to the object and displays a notification about the action.

This action is selected by default.

Allow download

If this action is selected, on detection of an infected object Web Anti-Virus allows the object to be downloaded to your computer.

General tab

In this window, the administrator can select the scan methods used by Web Anti-Virus, and configure the anti-phishing settings.

The following settings are available:

Check if web addresses are listed in the database of malicious web addresses

This check box enables / disables the option to scan web addresses against the database of malicious web addresses.

Checking web addresses against the database of malicious web addresses helps to detect websites that are in the black list of web addresses. The database of malicious web addresses is maintained by Kaspersky Lab, included in the application installation package, and updated during Kaspersky Endpoint Security database updates.

This check box is selected by default.

Heuristic analysis for detecting viruses

The check box enables / disables the use of heuristic analysis when scanning web traffic for viruses and other malware.

This check box is selected by default.

Slider

Moving the slider along the horizontal axis changes the heuristic analysis level of web traffic for viruses and other malicious programs. The heuristic analysis level ensures a balance between the thoroughness of scanning for threats, the load on the resources of the operating system, and the duration of heuristic analysis.

The following levels of heuristic analysis of web traffic for viruses and other malicious programs are available:

- **Light scan.** Heuristic Analyzer does not execute all instructions in executable files when scanning web traffic for malicious code. At this heuristic analysis level, the probability of detecting threats is lower than at the **medium scan** and **deep scan** heuristic analysis levels. Web traffic scanning is faster and less resource-intensive.
- **Medium scan.** When scanning web traffic for malicious code, Heuristic Analyzer performs the number of instructions in executable files that is recommended by Kaspersky Lab. This heuristic analysis level is selected by default.
- **Deep scan.** When scanning web traffic for malicious code, Heuristic Analyzer performs more instructions in executable files than at the **light scan** and **medium scan** levels of heuristic analysis. At this heuristic analysis level, the probability of detecting threats is

higher than at the **Light** and **Medium** levels of heuristic analysis. Web traffic scanning consumes more operating system resources and takes more time.

The slider is available if the **Heuristic analysis for detecting viruses** check box is selected.

Check if web addresses are listed in the database of phishing web addresses

This check box enables / disables the option to scan links to determine if they are in the database of phishing web addresses.

The database of phishing web addresses includes the web addresses of currently known websites that are used to launch phishing attacks. Kaspersky Lab supplements this database with web addresses that are obtained from the Anti-Phishing Working Group, an international organization. The database of phishing addresses is included in the application installation package and supplemented with Kaspersky Endpoint Security database updates.

The check box is selected by default.

Heuristic analysis for detecting phishing links

The check box enables / disables the use of heuristic analysis when scanning web pages for phishing links.

This check box is selected by default.

Trusted URLs tab

In this window, the administrator can form a list of trusted addresses from which web traffic will not be scanned.

The following settings are available:

Do not scan web traffic from trusted URLs

The check box enables / disables scanning of the content of web pages / websites whose addresses are included in the list of trusted web addresses.

If the check box is selected, Web Anti-Virus does not scan the content of web pages / websites whose addresses are included in the list of trusted web addresses.

If the check box is cleared, Web Anti-Virus scans the content of all opened web pages / websites.

This check box is selected by default.

Trusted web addresses

Contains the web addresses of web pages / websites whose content you trust. Web Anti-Virus does not scan the content of web pages / websites whose addresses are included in the list of trusted web addresses. You can add both the address and the address mask of a web page / website to the list of trusted addresses.

If the check box next to the web address of the web page / website is selected, Web Anti-Virus scans the content of the web page / website.

If the check box next to the URL of the web page / website is cleared, Web Anti-Virus temporarily excludes it from the list of trusted URLs and does not check its contents.

Add

This button opens the **Address / Address mask** window. In this window you can enter the address or address mask of the web page / website to be added to the list of trusted web addresses.

Edit

This button opens the **Address / Address mask** window. In this window, you can change the address or address mask of the web page / website that is added to the list of trusted web addresses.

The button is available if the address or address mask of the web page or website is selected.

Delete

This button removes the selected address or address mask of the web page / website from the list of trusted web addresses.

The button is available if the address or address mask of the web page or website is selected.

Web address / Web address mask window

In this window, the administrator can specify a web address or web address mask to be added to the trusted list.

The following settings are available:

Web address / Web address mask

Input field for the address or address mask of the web page / website.

For example, the address www.virus.com.

The following characters can be used to generate the address mask of the web page / website:

- * replaces any sequence of characters.

For example, Web Anti-Virus interprets the address mask `*abc*` as any web address that contains the sequence `abc` (for example, `www.virus.com/download_virus/page_0-9abcdef.html`).

- ? – Any single character.

For example, Web Anti-Virus interprets the address mask `Patch_123?.com` as any URL that contains the sequence `Patch_123?.com` and any character after the character 3 (for example, `patch_12345.com`).

If the URL contains the characters `*` and `?`, the `\` character needs to precede each of them. This is a special screening character, which indicates that the following character is to be interpreted not as a special symbol, but as any ordinary one. If the URL address includes the `\` character, it too must be preceded by the `\` character.

For example, `www.virus.com/download_virus/virus.dll\?virus_name=`.

Protection of IM client traffic. IM Anti-Virus

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about IM Anti-Virus and instructions on how to configure the component settings.

In this section:

About IM Anti-Virus	458
IM Anti-Virus section	459

About IM Anti-Virus

IM Anti-Virus scans the traffic of instant messaging clients (known as *IM clients*).

IM Anti-Virus does not scan messages transmitted over encrypted channels.

Messages that are sent through IM clients can contain the following kinds of security threats:

- URLs that attempt to download a malicious program to the computer
- URLs to malicious programs and websites that intruders use for phishing attacks

The goal of phishing attacks is to steal the personal data of users, such as bank card numbers, passport details, passwords for bank payment systems and other online services (such as social networking sites or email accounts).

Files can be transmitted through IM clients. When you attempt to save such files, they are scanned by the File Anti-Virus component (see section "About File Anti-Virus" on page [155](#)).

IM Anti-Virus intercepts every message that the user sends or receives through an IM client and scans it for links that may threaten the security of the computer:

- If no dangerous URLs are detected in the message, it becomes available to the user.
- If dangerous links are detected in the message, IM Anti-Virus replaces the message with information about the threat in the message window of the active IM client.

IM Anti-Virus section

IM Anti-Virus

Buttons  and 

The **Protection scope** section lets you select the type of messages that are transmitted by IM clients to be scanned by IM Anti-Virus.

Buttons  and 

Incoming and outgoing messages

If this setting is enabled, IM Anti-Virus scans both incoming and outgoing messages of IM clients for malicious objects or links that are in databases of suspicious and / or phishing web addresses.

This is the default setting.

Incoming messages only

The **Scan methods** section contains methods that IM Anti-Virus uses when scanning messages that arrive through IM clients.

Buttons  and 

Check if web addresses are listed in the database of malicious web addresses

Check if web addresses are listed in the database of phishing web addresses

This check box enables / disables scanning of web addresses in IM client messages against the database of phishing web addresses.

The Kaspersky Endpoint Security database of phishing web addresses includes websites that are known to be used in phishing attacks. Kaspersky Lab supplements this database with web addresses that are obtained from the Anti-Phishing Working Group, an international organization. The database of phishing web addresses is updated during Kaspersky Endpoint Security database updates.

This check box is selected by default.

System Watcher

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page [6](#)).

This section contains information about System Watcher and instructions on how to configure the component settings.

In this section:

About System Watcher.....	461
System Watcher section.....	462

About System Watcher

System Watcher collects data on the actions of applications on your computer and passes this information to other components for more reliable protection.

Behavior stream signatures

Behavior Stream Signatures (BSS) (also called "behavior stream signatures") contain sequences of application actions that Kaspersky Endpoint Security classifies as dangerous. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the specified action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

By default, if application activity fully matches a behavior stream signature, System Watcher moves the executable file of that application to Quarantine.

Rolling back actions that have been performed by malware

Based on information collected by System Watcher, Kaspersky Endpoint Security can roll back actions that have been performed by malware in the operating system while performing disinfection.

A rollback of malware actions can be initiated by File Anti-Virus (see page [155](#)) or during a virus scan (see section "Scanning the computer" on page [199](#)).

Rolling back malware operations affects a strictly defined set of data. Rollback has no adverse effects on the operating system or on the integrity of your computer data.

System Watcher section

System Watcher

This check box enables / disables the operation of the System Watcher component.

If the check box is selected, the functionality that is specified in the System Watcher settings is enabled.

If the check box is cleared, the functionality that is specified in the System Watcher settings is disabled.

This check box is selected by default.

Buttons and

Enable Exploit Prevention

This check box enables / disables the Exploit Prevention feature.

If the check box is selected, Kaspersky Endpoint Security keeps track of executable files launched by vulnerable applications. On detecting that an attempt to run an executable file from a vulnerable application was not initiated by the user, Kaspersky Endpoint Security blocks the launch of this file. Information about the blocked launch of the executable file is stored in the Exploit Prevention report.

This check box is selected by default.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of this setting in policies of a nested level of the hierarchy. All policies for nested administration groups and slave Administration Servers use the same setting value that is defined in the top-level policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of this setting in policies of a nested level of the hierarchy. On each client computer, Kaspersky Endpoint Security applies the setting value that is specified in policies for the nested administration groups or slave Administration Servers. The setting value does not depend on what is specified in the top-level policy.

The "lock" is closed by default.

The **Operating mode** section lets you configure the System Watcher settings for applications on client computers.



Do not monitor the activity of digitally signed applications

The check box enables / disables the function that adds digitally signed applications to the Trusted group.

The trust groups are as follows:

- **Trusted.** This group includes applications for which one or more of the following conditions are met:
 - applications are digitally signed by trusted vendors,
 - applications are recorded in the trusted applications database of Kaspersky Security Network,
 - the user has placed applications in the Trusted group.

No operations are prohibited for these applications.

- **Low Restricted.** This group includes applications for which the following conditions are met:

- applications are not digitally signed by trusted vendors,
- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is lower than 50,
- the user has placed applications in the "Low Restricted" group.

Such applications are subject to minimal restrictions on access to operating system resources.

- **High Restricted.** This group includes applications for which the following conditions are met:

- applications are not digitally signed by trusted vendors,
- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is in the 51-71 range,
- the user has placed applications in the High Restricted group.

Such applications are subject to high restrictions on access to operating system resources.

- **Untrusted.** This group includes applications for which the following conditions are met:

- applications are not digitally signed by trusted vendors,
- applications are not recorded in the trusted applications database of Kaspersky Security Network,
- the threat index of applications is in the 71-100 range,
- the user has placed applications in the Untrusted group.

Such applications are subject to high restrictions on access to operating system resources.

If the check box is selected, Kaspersky Endpoint Security adds digitally signed applications to the Trusted group. Kaspersky Endpoint Security does not monitor the activities of applications from this group.

If the check box is cleared, Kaspersky Endpoint Security does not add digitally signed applications to the Trusted group.

This check box is selected by default.

The **Action on threat detection** section lets you configure the settings for using behavior stream signatures (BSS).

Buttons  and 

On detecting malware activity

The items in this drop-down list determine the action that Kaspersky Endpoint Security performs on detection of malicious activity:

- **Select action automatically.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. By default, Kaspersky Endpoint Security moves the executable file of the malicious application to Quarantine.

This action is selected by default.

- **Move file to Quarantine.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security moves the executable file of this application to Quarantine.
- **Terminate the malicious program.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security terminates this application.
- **Skip.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security does not take any action on the executable file of the application.

The **Rollback of malware actions** section lets you enable or disable rollback of actions performed by malware in the system.

Buttons  and 

Roll back malware actions during disinfection

This check box enables / disables the function of Kaspersky Endpoint Security that allows rolling back malware actions in the operating system while disinfection is in progress.

If the check box is selected, Kaspersky Endpoint Security rolls back malware actions in the operating system while disinfection is in progress.

This check box is selected by default.

Advanced application settings

This section describes advanced settings of Kaspersky Endpoint Security and how they can be configured.

In this section:

Application settings section	467
KSN settings section	481
Interface section.....	484

Application Settings section

The **Self-Defense Settings** section lets you configure protection against external interference with the operation of the computer.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Enable Self-Defense

This check box enables / disables Kaspersky Endpoint Security Self-Defense, which prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

When this check box is selected, Kaspersky Endpoint Security prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

This check box is selected by default.

Disable external management of the system service

This check box enables / disables Remote Control Defense, which blocks any attempts to remotely manage Kaspersky Endpoint Security services.

When the check box is selected, Kaspersky Endpoint Security blocks all attempts to manage application services from a remote computer. When an attempt is made to manage application services remotely, a notification is displayed in the Microsoft Windows taskbar, above the application icon (unless the notification service has been disabled by the user).

This check box is selected by default.

The **Operating mode** section lets you configure optimum energy and computer resource consumption in the operation of Kaspersky Endpoint Security.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Settings

Clicking this button opens the **Operating mode** window.

The **Proxy Server Settings** section allows you to configure the connection to a proxy server that you use to access the Internet.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Settings

Clicking the button opens the **Proxy server settings** window. This window lets you configure proxy server settings.

The **Password protection** section lets you configure the password scope.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Settings

This button opens the **Password protection** window. This window lets you configure the password scope.

The **Background scan** section lets you configure a virus scan to pause during activity by the user on the client computer with Kaspersky Endpoint Security installed.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Perform Idle Scan

This check box enables / disables an option that starts a scan task for autorun objects, RAM, and the operating system partition when the computer is locked or the screensaver is on for 5 minutes or longer, if one of the following conditions is true:

- An idle scan of the computer has not been performed since installation of Kaspersky Endpoint Security.
- The previous idle scan of the computer was completed more than 7 days ago.
- The previous idle scan of the computer was interrupted during an update of the application databases and modules.
- The previous idle scan of the computer was interrupted during an on-demand scan.

If the check box is selected, the idle scan task starts when one of the preceding conditions is true.

If the check box is cleared, the idle scan task does not start.

This check box is cleared by default.

The **Scan removable drives on connection** section lets you select the action that Kaspersky Endpoint Security performs when you connect removable drives to the computer.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Action on removable drive connection

This drop-down list lets you select the action that Kaspersky Endpoint Security performs when a removable drive is connected to the computer.

The drop-down list contains the following items:

- **Do not scan**

If this item is selected, Kaspersky Endpoint Security does not scan the removable drive.

This item is selected by default.

- **Detailed Scan**

If this item is selected, after a removable drive is connected Kaspersky Endpoint Security scans all files located on the removable drive, including files within compound objects.

- **Quick Scan**

If this item is selected, when a removable drive is connected Kaspersky Endpoint Security scans only files with specific extensions that are most vulnerable to infection, and does not unpack compound objects.

com – executable file of an application no larger than 64 KB

exe – executable file or self-extracting archive

sys – Microsoft Windows system file

prg – program text for dBase™, Clipper or Microsoft Visual FoxPro®, or a WAVmaker program

bin – binary file

bat – batch file

cmd – command file for Microsoft Windows NT (similar to a bat file for DOS), OS/2

dpl – compressed Borland Delphi library

dll – dynamic link library

scr – Microsoft Windows splash screen

cpl – Microsoft Windows control panel module

ocx – Microsoft OLE (Object Linking and Embedding) object

tsp – program running in split-time mode

drv – device driver

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – Microsoft Windows link file

reg – Microsoft Windows system registry key file

ini – configuration file which contains configuration data for Microsoft Windows, Windows NT, and some applications

cla – Java class

vbs – Visual Basic® script

vbe – BIOS video extension

js, jse – JavaScript source text

htm – hypertext document

htt – Microsoft Windows hypertext header

hta – hypertext program for Microsoft Internet Explorer®

asp – Active Server Pages script

chm – compiled HTML file

pht – HTML file with integrated PHP scripts

php – script that is integrated into HTML files

wsh – Microsoft Windows Script Host file

wsf – Microsoft Windows script

the – Microsoft Windows 95 desktop wallpaper file

hlp – Win Help file

eml – Microsoft Outlook Express message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – extension for saved Microsoft Office Outlook emails

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file. Next generation of Microsoft Windows OS metafiles. EMF files are not supported by 16-bit Microsoft Windows.

ico – object icon file

ov? – Microsoft Office Word executable files

xl* – Microsoft Office Excel documents and files, such as: xla, the extension for Microsoft Office Excel, xlc for diagrams, xlt for document templates,.xlsx for Microsoft Office Excel 2007 workbooks, xltm for Microsoft Office Excel 2007 workbooks with macro support, xlsb for Microsoft Office Excel 2007 workbooks in binary (non-XML) format, xltx for Microsoft Office Excel 2007 templates, xism for Microsoft Office Excel 2007 templates with macro support, and xlam for Microsoft Office Excel 2007 plug-ins with macro support

pp* – Microsoft Office PowerPoint® documents and files, such as: pps for Microsoft Office PowerPoint slides, ppt for presentations, pptx for Microsoft Office PowerPoint 2007 presentations, pptm for Microsoft Office PowerPoint 2007 presentations with macros support, potx for Microsoft Office PowerPoint 2007 presentation templates, potm for Microsoft Office PowerPoint 2007 presentation templates with macro support, ppsx for Microsoft Office PowerPoint 2007 slide shows, ppsm for Microsoft Office PowerPoint 2007 slide shows with macro support, and ppam for Microsoft Office PowerPoint 2007 plug-ins with macro support

md* – Microsoft Office Access® documents and files, such as: mda for Microsoft Office Access workgroups and mdb for databases

sldx – a Microsoft PowerPoint 2007 slide

sldm – a Microsoft PowerPoint 2007 slide with macro support

Maximum removable drive size

This check box enables / disables a limit on the size of removable drives on connection of which Kaspersky Endpoint Security performs the action that is selected in the **Actions on removable drive connection** drop-down list.

If this check box is selected, Kaspersky Endpoint Security performs the action that is selected in the **Actions on removable drive connection** drop-down list on removable drives with a size not more than the specified maximum drive size.

If the check box is cleared, Kaspersky Endpoint Security performs the action that is selected in the **Actions on removable drive connection** drop-down list on removable drives of any size.

Removable drive size is specified in megabytes. The default value is 4096 MB.

This setting is available if the **Full Scan** or **Quick Scan** action is selected in the **Actions on removable drive connection** drop-down list.

This check box is cleared by default.

Proxy Server Settings window

In this window, the administrator can configure proxy server settings.

The following settings are available:

Use proxy server

This check box enables / disables the use of a proxy server for Internet connections by Kaspersky Endpoint Security.

If the check box is selected, the group of settings of the proxy server is available for configuration. Kaspersky Endpoint Security uses these settings for certain protection components, including for updating databases and application modules.

This check box is selected by default.

Automatically detect proxy server settings

If this setting is selected, Kaspersky Endpoint Security detects the address of the proxy server automatically by using the WPAD (Web Proxy Auto-Discovery) protocol. If the IP address of the proxy server cannot be determined by using this protocol, Kaspersky Endpoint Security uses the proxy server address that is specified in Microsoft® Internet Explorer®.

This setting is available if the **Use proxy server** check box is selected.

This is the default setting.

Use specified proxy server address and port

If this setting is selected, Kaspersky Endpoint Security uses the address and the port of the proxy server that are specified below in the **Address** field and in the **Port** field.

This setting is available if the **Use proxy server** check box is selected.

Address

Field for entering the IP address or symbolic name of a proxy server.

For example, the IP address 192.168.0.1.

The field is available if the **Use specified proxy server address and port** setting is selected.

Port

Field for entering the port number of a proxy server.

The field is available if the **Use specified proxy server address and port** setting is selected.

By default, port number 80 is specified.

Set user name and password for authentication

Authentication is the process of verifying user registration data for access control purposes.

This check box enables / disables the use of authentication on the proxy server.

If the check box is selected, Kaspersky Endpoint Security first tries NTLM and then BASIC authorization on the proxy server, with the data that is specified in the **User name** and **Password** fields.

If the check box is cleared, Kaspersky Endpoint Security attempts NTLM authorization with data for the account under which the task (such as an update task) is running.

If the proxy server requires authentication and no user name and password are specified, or the specified data was not accepted by the proxy server for any reason, a window is displayed, prompting you for a user name and password. If authentication is completed successfully, Kaspersky Endpoint Security uses the specified user name and password in the future. Otherwise, Kaspersky Endpoint Security prompts you for the authentication settings again.

The check box is available if the **Use proxy server** check box is selected.

This check box is cleared by default.

User name

Field for entering the user name that is used for authentication on the proxy server.

The file is available if the **Set user name and password for authentication** check box is selected.

Password

Field for entering the user password that is used for authentication on the proxy server.

The file is available if the **Set user name and password for authentication** check box is selected.

Bypass proxy server for local addresses

This check box enables / disables the use of a proxy server when Kaspersky Endpoint Security performs an update from a shared folder.

If the check box is selected, Kaspersky Endpoint Security does not use a proxy server when performing an update from a shared folder.

The check box is available if the **Use proxy server** check box is selected.

This check box is selected by default.

Password protection window

The **Password** section lets you specify a password for managing all or some functions and settings of Kaspersky Endpoint Security. This password will be used to associate users with Administrator permissions in local GUI or command line operations.

User name

A field for entering the user name to appear in the entries about events involving operations performed with Kaspersky Endpoint Security.

New password

A field for entering a password to be used for subsequent access to Kaspersky Endpoint Security.

Password confirmation

A field for confirming the password that is typed in the **New password** field.

To ensure high level of security password should meet current industry recommended complexity requirements or be a 10 + length set of random characters, including alphanumeric and special symbols.

The **Password scope** section lets you specify which operations cannot be performed until the defined password is entered.

Application settings configuration

The check box enables / disables requests for the password when the user attempts to save changes to the application settings.

When this check box is selected, Kaspersky Endpoint Security prompts the user for a password before saving changes to settings.

This check box is cleared by default.

Closing the application

The check box enables / disables requests for the password when the user attempts to quit the application.

If the check box is selected, Kaspersky Endpoint Security prompts the user to enter the password when the user attempts to close the application.

This check box is cleared by default.

Disable protection components

The check box enables / disables the user name and password prompt when the user attempts to disable protection components.

If the check box is selected and the user attempts to disable any one of the protection components, Kaspersky Endpoint Security prompts the user to enter the user name and password.

The following components are protection components:

- File Anti-Virus
- System Watcher
- Mail Anti-Virus
- Web Anti-Virus
- IM Anti-Virus
- Firewall
- Network Attack Blocker
- BadUSB Attack Protection.

Disabling control components

The check box enables / disables the user name and password prompt when the user attempts to disable application control components.

If the check box is selected and the user attempts to disable any application component, Kaspersky Endpoint Security prompts the user to enter the user name and password.

The following components are control components:

- Application Startup Control
- Application Privilege Control
- Vulnerability Monitor
- Device Control
- Web Control

Key removal

This check box enables / disables the password prompt when the user attempts to remove the application key.

If the check box is selected and the user attempts to remove a key, Kaspersky Endpoint Security prompts the user to enter a password.

This check box is cleared by default.

Remove / modify / restore the application

This check box enables / disables the password prompt on the user's attempt to remove, modify, or restore the application.

If the check box is selected and the user attempts to remove, modify, or repair the application, Kaspersky Endpoint Security prompts the user to enter a password.

This check box is cleared by default.

Restoring access to data on encrypted drives

This check box enables / disables the password prompt that is shown when the user attempts to restore access to data on encrypted drives.

If the check box is selected and the user attempts to restore access to data on encrypted drives, Kaspersky Endpoint Security prompts the user to enter a password.

This check box is cleared by default.

Viewing reports

This check box enables / disables the user name and password prompt when the user attempts to open the **Reports** window.

If the check box is selected and the user attempts to open the **Reports** window, Kaspersky Endpoint Security prompts the user to enter the user name and password.

Select all

Clicking this button lets you select the check boxes opposite all operations. All operations with the application will be password protected.

Clear all

Clicking this button lets you clear the check boxes opposite all operations. No operations with the application will be password protected.

The **Temporary password** section lets you configure the settings for use of a temporary password to provide a user with the capability to perform specific operations for a limited amount of time. This section is available when the **Password protection** window is opened from the computer properties window.

Settings

Clicking this button opens the **Create temporary password** window. In this window, you can specify the expiration date and the scope of the temporary password.

KSN Settings section

The **KSN Settings** section lets you view the KSN Participation Statement and confirm your consent or decline to participate in the KSN program.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

I accept the terms of the Agreement and would like to participate in KSN

The check box enables / disables the use of Kaspersky Security Network (KSN) in the operation of Kaspersky Endpoint Security. The use of KSN is voluntary.

If the check box is selected, information about the reputation of files, web resources, and application received from KSN databases is used in the operation of Kaspersky Endpoint Security components.

If the check box is cleared, only information stored in local application databases is used in the operation of Kaspersky Endpoint Security.

If the check box was selected during initial configuration of Kaspersky Endpoint Security, this check box remains selected. If the check box was cleared, it remains cleared.

KSN Participation Agreement

Clicking this link opens the **Global KSN** or **Private KSN** window depending on the KSN provider. You can review the terms of the Kaspersky Security Network Statement in this window.

The **KSN Proxy Settings** section lets you configure the KSN Proxy settings.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Use KSN Proxy

The check box enables / disables use of *KSN Proxy*. KSN Proxy is a service that facilitates interaction between the infrastructure of Kaspersky Security Network and client computers that are managed by Administration Server.

If the check box is selected, KSN Proxy is being used.

This check box is selected by default.

Use KSN servers when KSN Proxy is not available

The check box enables / disables use of KSN servers if the KSN Proxy service is not available. KSN servers may be located both on the side of Kaspersky Lab (when Global KSN is used) and on the side of third parties (when Private KSN is used).

The check box is available if the **Use KSN Proxy** check box is selected.

This check box is cleared by default.

The **Notifications about the availability of KSN servers** section lets you configure the Administration Console to display the statuses of client computers with Kaspersky Endpoint Security installed.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Computer status when KSN servers are not available. The items in this drop-down list determine which computer status is displayed in the Administration Console when KSN servers are not available.

You can select the following list items:

- **OK.**
- **Warning.**
- **Critical.**

The **Warning** item is selected by default.

Interface section

The **Interaction with user** section lets you configure the display of the application interface on client computers with Kaspersky Endpoint Security installed.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Show application interface

The check box enables / disables the display of the Kaspersky Endpoint Security interface.

If this check box is selected, a user who works on a client computer with Kaspersky Endpoint Security installed sees the folder with the application name in the **Start** menu, the Kaspersky Endpoint Security icon in the taskbar notification area of Microsoft Windows, and pop-up notifications. The user can also view and, depending on the available permissions, configure application settings from the application interface.

When this check box is cleared, a user who works on a client computer with Kaspersky Endpoint Security installed does not see any signs of Kaspersky Endpoint Security operation, including the animation of the application icon when tasks are running.

This check box is selected by default.

The **Warnings** section lets you configure which application messages must be displayed on the Kaspersky Endpoint Security icon in the notification area.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Unprocessed files

This check box enables / disables the display of messages about unprocessed files on client computers that have Kaspersky Endpoint Security installed.

If the check box is selected, the user operating on the client computer with Kaspersky Endpoint Security installed sees a pop-up notification about unprocessed files in the Microsoft Windows taskbar notification area.

If the check box is cleared, a notification about unprocessed files is not displayed.

This check box is selected by default.

Computer restart required

This check box enables / disables the display of notifications about the need to restart client computers that have Kaspersky Endpoint Security installed.

If the check box is selected, the user operating on the client computer with Kaspersky Endpoint Security installed sees a computer restart required pop-up notification in the Microsoft Windows taskbar notification area.

If the check box is not selected, a computer restart required notification is not displayed.

This check box is selected by default.

Problems with antivirus databases

This check box enables / disables the display of messages about problems with antivirus databases on client computers that have Kaspersky Endpoint Security installed.

If the check box is selected, the user operating on the client computer with Kaspersky Endpoint Security installed sees a pop-up notification about problems with antivirus databases in the Microsoft Windows taskbar notification area.

If the check box is cleared, a notification about problems with antivirus databases is not displayed.

This check box is selected by default.

Problems with protection level

This check box enables / disables the display of messages about problems with the protection level on client computers with Kaspersky Endpoint Security installed.

If the check box is selected, the user operating on the client computer with Kaspersky Endpoint Security installed sees a pop-up notification about problems with the protection level in the Microsoft Windows taskbar notification area.

If the check box is cleared, a notification about problems with the protection level is not displayed.

This check box is selected by default.

Problems with license

This check box enables / disables the display of notifications about licensing issues on client computers that have Kaspersky Endpoint Security installed.

If the check box is selected, the user operating on the client computer with Kaspersky Endpoint Security installed sees a pop-up notification about licensing issues in the Microsoft Windows taskbar notification area.

If the check box is cleared, a notification about licensing issues is not displayed.

This check box is selected by default.

Updates available

This check box enables / disables the display of messages about available updates on client computers that have Kaspersky Endpoint Security installed.

If the check box is selected, the user operating on the client computer with Kaspersky Endpoint Security installed sees a pop-up notification about available updates in the Microsoft Windows taskbar notification area.

If the check box is cleared, a notification about available updates is not displayed.

This check box is selected by default.

The **User support** section lets you create a list of links to web resources containing information about technical support for Kaspersky Endpoint Security.



The button with the closed "lock" means that Kaspersky Security Center blocks editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of settings, i.e. the values that are specified in the policy.

The button with the open "lock" means that Kaspersky Security Center allows editing of the settings of this section from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of settings.

The "lock" is closed by default.

Settings (Support information). Clicking this button opens the **Support information** window. This window lets you create links to web resources containing information about technical support for Kaspersky Endpoint Security. Links that are created in this window are displayed in the **Support** window of the Kaspersky Endpoint Security local interface instead of standard links.

Support information window

In this window, the administrator can specify the links to web resources that will be available to the user in the local interface of Kaspersky Endpoint Security in the **Support** window.

The following settings are available:

Description

Field for entering any information and notes.

Add

Clicking this button opens the **Link to web resource** window. This window lets you enter the details of Technical Support web resources. These links will be displayed in the **Support** window of the Kaspersky Endpoint Security local interface instead of the default links.

Edit

Clicking this button opens the **Link to web resource** window. This window lets you edit web resource details.

This button is active when an item is selected in the list of links to web resources.

Delete

Clicking this button deletes the link to a web resource.

This button is active when an item is selected in the list of links to web resources.

Move up

Clicking this button moves the web resource that is selected in the table one line up. Links will be displayed in the **Support** window of the Kaspersky Endpoint Security local interface in the same order that is set in the **Links to web resources** table.

This button is available when the top item is not selected in the **Links to web resources** table.

Move down

Clicking this button moves the web resource that is selected in the table one line down. Links will be displayed in the **Support** window of the Kaspersky Endpoint Security local interface in the same order that is set in the **Links to web resources** table.

This button is available when the lowest item is not selected in the **Links to web resources** table.

Links to web resources. Table in which you can add links to Technical Support web resources. If the table is empty, the default links are displayed in the Kaspersky Endpoint Security local interface.

The table contains the following columns:

- **Name.** This column displays the name of the web resource.

- **Address.** This column displays the address of the web resource.
- **Description.** This column contains a description of the web resource.

Tasks

This section describes how to manage tasks for Kaspersky Endpoint Security. View the *Kaspersky Security Center Administrator's Guide* for details on task management through Kaspersky Security Center.

In this section:

About tasks for Kaspersky Endpoint Security	489
Key addition task settings section	491
Application components modification task settings section.....	493
Authentication Agent account management task settings section	495
Settings section.....	496

About tasks for Kaspersky Endpoint Security

Kaspersky Security Center controls the activity of Kaspersky Lab applications on client computers by means of tasks. Tasks implement the primary administrative functions, such as key installation, computer scanning, and database and application software module updates.

You can create the following types of tasks to administer Kaspersky Endpoint Security through Kaspersky Security Center:

- Local tasks that are configured for an individual client computer.
- Group tasks that are configured for client computers within administration groups.

- Tasks for a set of computers that do not belong to administration groups.

Tasks for sets of computers outside of administration groups apply only to the client computers that are specified in the task settings. If new client computers are added to a set of computers for which a task is configured, this task does not apply to these new computers. To apply the task to these computers, create a new task or edit the settings of the existing task.

To remotely manage Kaspersky Endpoint Security, you can use the following tasks of any of the listed types:

- **Add key.** Kaspersky Endpoint Security adds a key for application activation, including an additional key.
- **Change application components.** Kaspersky Endpoint Security installs or removes components on client computers according to the list of components specified in the task settings.
- **Inventory.** Kaspersky Endpoint Security collects information about all application executable files that are stored on computers.

You can enable inventory of DLL modules and script files. In this case, Kaspersky Security Center will receive information about DLL modules loaded on a computer with Kaspersky Endpoint Security installed, and about files containing scripts.

Enabling inventory of DLL modules and script files significantly increases the inventory task duration and the database size.

- **Update.** Kaspersky Endpoint Security updates databases and application modules according to the configured update settings.
- **Rollback.** Kaspersky Endpoint Security rolls back the last update of databases and modules.
- **Virus scan.** Kaspersky Endpoint Security scans the computer areas specified in the task settings for viruses and other threats.

- **Checking connection with KSN.** Kaspersky Endpoint Security sends a query about the availability of KSN servers and updates the KSN connection status.
- **Integrity Check.** Kaspersky Endpoint Security receives data about the set of application modules installed on the client computer and scans the digital signature of each module.
- **Manage Authentication Agent accounts.** While performing this task, Kaspersky Endpoint Security generates commands for removing, adding, or modifying Authentication Agent accounts.

You can perform the following actions with tasks:

- Start, stop, suspend, and resume tasks.
- Create new tasks.
- Edit task settings.

The rights to access the settings of Kaspersky Endpoint Security tasks (read, write, execute) are defined for each user who has access to Kaspersky Security Center Administration Server, through the settings of access to functional areas of Kaspersky Endpoint Security. To configure access to the functional areas of Kaspersky Endpoint Security, go to the **Security** section of the properties window of Kaspersky Security Center Administration Server.

Key addition task settings section

In this window, the administrator can configure the task settings for adding a key to client computers that have Kaspersky Endpoint Security installed.

The following settings are available:

Activation code

If this add key option is selected, the application activation code entry field becomes available.

Select

Clicking this button opens the **List of activation codes in Kaspersky Security Center storage** window. This window lets you choose an activation code from the Kaspersky Security Center storage.

Key file or key

If this add key option is selected, the **Select** drop-down button becomes available. This button lets you select a key file based on which the key will be added, or select a key that has already been added to Kaspersky Security Center key storage.

Select

This button opens the button context menu with the following items:

- **Key file from folder.** Selecting this item opens the **Select key file** window. This window lets you specify the path to the key file with the `key` extension, based on which the key will be added.
- **Key from Kaspersky Security Center storage.** Selecting this item opens the **List of keys in Kaspersky Security Center storage** window. This window lets you choose a key from the Kaspersky Security Center key storage.

Add this key as an additional key

This check box enables / disables the option of adding the selected key file as an additional key.

If this check box is selected, Kaspersky Endpoint Security uses the selected key file as an additional license key file, postponing the installation of the key file until the current license expires.

If this check box is cleared, Kaspersky Endpoint Security uses the selected key file as the key to the current license by installing the selected key file when the key file installation task is performed.

This check box is cleared by default.

Information about the key

A group of settings for the license that is installed on a computer or computers as a result of the key file installation task:

- **Key file status.**

- **License number.**
- **License type.** Possible options: commercial or trial.
- **License term.** Number of days until the key expires.
- **Key file expires.** Date of key file expiration.

Application components modification task settings section

In this window, the administrator can configure the task settings for modifying the set of components on client computers that have Kaspersky Endpoint Security installed.

The following components are available:

Type of installation

Drop-down list letting you specify the type of Kaspersky Endpoint Security installation. Possible items in the list:

- **Basic installation.** If you choose this type of installation, the basic protection components with settings recommended by Kaspersky Lab are installed on the computer.
- **Standard installation.** If you choose this type of installation, the protection and control components with settings recommended by Kaspersky Lab are installed on the computer.
- **Full installation.** If you choose this type of installation, all application components with settings recommended by Kaspersky Lab are installed on the computer.

Basic installation is selected by default.

Components to install

The check box next to the name of an application component includes the component in the installation / removal list.

If the check box opposite the name of a component is selected, Kaspersky Endpoint Security installs the component while performing the task. If the component is already installed, no changes are made to the set of components.

If the check box opposite the name of a component is cleared, Kaspersky Endpoint Security removes the component while performing the task. If the component has not yet been installed, no changes are made to the set of components.

You cannot clear the check box for the File Anti-Virus component.

Remove incompatible third-party software

This check box enables / disables the option whereby Kaspersky Endpoint Security removes incompatible third-party software from the user's computer.

This check box is selected by default.

Additional

This button opens the **Advanced Settings** window. This window lets you set a password for modifying the set of application components.

Settings section

In this window, the administrator can configure the settings of a user account whose permissions let the user modify the set of components on client computers that have Kaspersky Endpoint Security installed.

The following settings are available:

Set password for modifying the set of application components

This check box enables / disables the prompt for a password when a user attempts to remove or install any component on the client computer.

This check box is cleared by default.

User name

Field for entering the name of the user possessing the right to modify the set of application components.

Password. Field for entering the account password for obtaining the right to modify the set of application components.

Authentication Agent account management task settings section

In this window, the administrator can configure the settings for the Authentication Agent account management task.

The following settings are available:

Commands for managing Authentication Agent accounts

Table with a list of commands for adding, editing, and deleting Authentication Agent accounts. The table contains the following columns:

User name

This column shows the name of an Authentication Agent account and an icon reflecting the nature of the command: adding, deleting or editing the Authentication Agent account.

Certificate-based authentication

This column shows information on whether or not authentication using a token or smart-card is allowed.

Password-based authentication

This column shows information on whether or not authentication using an Authentication Agent account name and password is allowed.

Add

This button opens the button context menu with the following items:

- **Account adding command.** Selecting this item opens the **Add user account** window. This window lets you specify the user account settings that Kaspersky Endpoint Security uses when creating an Authentication Agent account.
- **Account editing command.** Selecting this item opens the **Edit user account** window. This window lets you edit the settings of an existing Authentication Agent account. The settings will be edited when the task is performed.
- **Account deletion command.** Selecting this item opens the **Delete user account** window. This window lets you specify an Authentication Agent account that you want to delete from the list of Authentication Agent accounts.

Edit

Clicking this button opens a window. This window lets you edit the command selected in the **Commands for managing Authentication Agent accounts** table.

This button is available if a command is selected in the **Commands for managing Authentication Agent accounts** table.

Delete

Clicking this button deletes a command from the **Commands for managing Authentication Agent accounts** table.

This button is available if a command is selected in the **Commands for managing Authentication Agent accounts** table.

Settings section

In the **Security level** section, you can select one of the three file security levels that have been created by Kaspersky Lab specialists, or configure file security level settings on your own. When deciding on a file security level, be sure to take working conditions and the current situation into account.

High

If the probability of computer infection is very high, select this file security level.

Kaspersky Endpoint Security scans all types of files. When scanning compound files, Kaspersky Endpoint Security also scans mail-format files.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists.

Kaspersky Endpoint Security scans only the specified file formats on all hard drives, network drives, and removable storage media of the computer, and also embedded OLE objects.

Kaspersky Endpoint Security does not scan archives or installation packages.

The **Recommended** file security level is selected by default.

Low

The settings of this file security level ensure maximum scanning speed.

Kaspersky Endpoint Security scans only new or modified files with the specified extensions on all hard drives, removable drives, and network drives of the computer. Kaspersky Endpoint Security does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

By default

This button sets the file security level to **Recommended**.

Settings (Scan scope)

Clicking this button opens the **Objects to scan** window. This window lets you specify the objects to be scanned by Kaspersky Endpoint Security during the virus scan task.

Suspend scheduled scanning when the screensaver is off and the computer is unlocked

This check box enables / disables a function that suspends the start of the scan task when computer resources are limited. Kaspersky Endpoint Security starts the scan task when the screensaver is on and the computer is locked.

This check box is cleared by default.

The **Action on threat detection** section lets you select the action that Kaspersky Endpoint Security performs after a virus scan detects infected or probably infected files.

Select action automatically

If this option is selected, Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. This action is **Select action: Disinfect. Delete if disinfection fails**.

Perform action: Disinfect. Delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

To select the **Perform action: Disinfect. Delete if disinfection fails** action, select the **Perform action** setting and select the **Disinfect** and **Delete if disinfection fails** check boxes.

This action is selected by default.

Perform action: Disinfect

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected or probably infected files that are detected. If disinfection fails, Kaspersky Endpoint Security moves them to Quarantine.

To select the **Perform action: Disinfect** action, select the **Perform action** setting, select the **Disinfect** check box, and clear the **Delete if disinfection fails** check box.

Perform action: Delete

If this option is selected, Kaspersky Endpoint Security automatically deletes all infected or probably infected files that are detected.

To select the **Perform action: Delete** action, select the **Perform action** setting, clear the **Disinfect** check box, and select the **Delete** check box.

Perform action: Inform

If this option is selected, on detecting infected or probably infected files Kaspersky Endpoint Security informs you of this and moves the detected files to Quarantine.

To select the **Perform action: Inform** action, select the **Perform action** setting and clear the **Delete if disinfection fails** and **Disinfect** check boxes.

Perform Advanced Disinfection immediately

Managing the application from the command prompt

This section contains a description of how to work with Kaspersky Endpoint Security from the command line.

In this section:

Commands.....	499
Error messages.....	509
Return codes.....	515
Using task profiles.....	526

Commands

The following commands are available for working with the application from the command line:

Table 1. Commands for working with the application

Commands	Action
HELP	Show Help.
SCAN	Run the virus scan task.
UPDATE	Update the anti-virus databases and application modules.
ROLLBACK	Roll back the last anti-virus database update.
TRACES	Enable / disable tracing.
START	Run the task.
STOP	Stop the running task.
STATUS	Show the task status.
STATISTICS	Show the task execution statistics.
RESTORE	Restore the file from Quarantine.
EXPORT	Export application settings.
IMPORT	Import application settings.
ADDKEY	Add a key.
LICENSE	Perform operations with a license.
PBATESTRESET	Delete information about the compatibility of the system hard drive and Authentication Agent (for more detailed information, please refer to the <i>Administrator's Guide</i>).
EXIT	close the application
EXITPOLICY /password=<password>	Disable a Kaspersky Security Center policy (password-protected operation).

Commands	Action
STARTPOLICY	Enable a Kaspersky Security Center policy that was disabled using the EXITPOLICY command.
RENEW	Open the web page for purchasing licenses in the browser.
DISABLE	Disable File Anti-Virus (the license status is checked prior to execution).
CLS	Clear the console screen.
SPYWARE	Enable or disable detection of spyware.
MESSAGES <on off>	Enable or disable interactive mode.
PATCHCOMPATIBILITYRES ET GUID1 GUID2 ...	Delete patches with IDs of GUID1, GUID2, etc. from the list of incompatible patches.

SCAN command

Use:

```
SCAN [<files>] [/ALL] [/MEMORY] [/STARTUP] [/MAIL] [/REMDRIVES]
[/FIXDRIVES] [/NETDRIVES] [/QUARANTINE] [/@:<filelist.lst>]
[/i<0-4>] [-e:a|s|b|<filemask>|<seconds>]
[/R[A]:<report_file>] [/C:<settings_file>]
SCAN /VLNS2 [/WUA] [/WSUSCAB <wsus_file>] [<files>] [/lst
<filelist.lst>]
```

Scanning for vulnerabilities:

- /VLNS2 - scan for vulnerabilities.
- /WUA - scan using WUA (disabled by default).
- /WSUSCAB <wsus_file> - specify the WSUS file.

Scan scope:

- `<files>` - list of files and folders separated by blank spaces (long paths must be enclosed in quotation marks).
- `/ALL` - scan the computer.
- `/MEMORY` - scan computer memory.
- `/STARTUP` - scan startup objects.
- `/MAIL` - scan mailboxes.
- `/REMDRIVES` - scan removable drives.
- `/FIXDRIVES` - scan hard drives.
- `/NETDRIVES` - scan network drives.
- `/QUARANTINE` - scan quarantined files.
- `/@:<filelist.lst>` - scan files that are in the specified list.

Actions to perform on detected objects:

- `/i0` - notify.
- `/i1` - disinfect or skip if disinfection fails.
- `/i2` - disinfect or delete if disinfection fails (in this case, the application does not delete files from containers but deletes containers that have an executable extension).
- `/i3` - disinfect or delete if disinfection fails (in this case, the application deletes containers if it is impossible to delete the object from a container).
- `/i4` - delete (including deletion of containers if it is impossible to delete the object from a container).
- `/i8` (default) - immediately ask the user.
- `/i9` - ask the user after the task completes.

Scan mode:

- `/fe` - fast (by extension).
- `/fi` - smart (by format).
- `/fa` (default) - full (all files are scanned).

Exclusions:

- `-e:a` - skip archives.
- `-e:b` - skip mail databases and the text of email messages.
- `-e:<filemask>` - skip files by mask.
- `-e:<seconds>` - skip files that are scanned for longer than the specified amount of `<seconds>`.
- `-es:<size>` - skip files that are larger than the specified amount of `<megabytes>`.

Reports:

- `/R:<report_file>` - save only critical events to the report.
- `/RA:<report_file>` - save all events to the report.

Advanced settings:

- `/iChecker=<on|off>` - enable or disable iChecker technology.
- `/iSwift=<on|off>` - enable or disable iSwift technology.
- `/C:<settings_file>` - specify the configuration file.

Examples:

- `avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files" C:\Downloads\test.exe`

- `avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log`
- `avp.com SCAN /VLNS2`
- `avp.com SCAN /VLNS2 /RA:scan.log /WUA C:\Windows\`

UPDATE command

Use:

```
UPDATE [source] [/R[A]:<report_file>] [/C:<settings_file>]
```

Parameters:

- `source` - web address or path to the local folder of the update source.
- `/R:<report_file>` - save only critical events to the report.
- `/RA:<report_file>` - save all events to the report.
- `/C:<settings_file>` - specify the configuration file.

Examples:

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK command

Use:

```
ROLLBACK /login=<login> /password=<password> [/R[A]:<report_file>]
```

Parameters:

- `/R:<report_file>` - save only critical events to the report.
- `/RA:<report_file>` - save all events to the report.

Examples:

```
avp.com ROLLBACK /RA:rollback.txt
```


TRACES command

Use:

```
TRACES on/off [<trace_level>] [all|dbg|file]
```

Parameters:

- on - enable tracing.
- off - disable tracing.
- <trace_level> - level of detail of tracing (available values: 100, 200, 300, 400, 500, 600).
- all - use the `OutputDebugString` function and save the trace file.
- dbg - use the `OutputDebugString` function to display the trace file.
- file - save the trace file.

Examples:

- `avp.com TRACES on 500`
- `avp.com TRACES on 500 dbg`
- `avp.com TRACES off`
- `avp.com TRACES 500`
- `avp.com TRACES off file`

START command

Use:

```
START <Profile> [/R[A]:<report_file>]
```

Parameters:

- <Profile> - profile name.
- /R:<report_file> - save only critical events to the report.
- /RA:<report_file> - save all events to the report.

Get list of available profiles: avp.com HELP START

Examples:

```
avp.com START Scan_Objects
```

STOP command

Use:

```
STOP <Profile> /login=<login> /password=<password>
```

<Profile> parameter - profile name.

Get list of available profiles: avp.com HELP STOP

STATUS command

Use:

```
STATUS [Profile]
```

Get list of available profiles: avp.com HELP STATUS

STATISTICS command

Use:

```
STATISTICS <Profile>
```

-

RESTORE command

Use:

```
RESTORE [/REPLACE] <filename>
```

Parameters:

- /REPLACE - overwrite the existing file.
- <filename> - name of the restored file.

Examples:

```
avp.com RESTORE /REPLACE C:\eicar.com
```

EXPORT command

Use:

```
EXPORT <Profile> <filename>
```

Parameters:

- <Profile> - name of the profile whose settings need to be exported.
- <filename> - name of the file to which the settings need to be exported.

Use the TXT extension for files in text format.

Examples:

- avp.com EXPORT rtp rtp_settings.dat - binary export
- avp.com EXPORT fm fm_settings.txt - plain export

Get list of available profiles: avp.com HELP EXPORT

:

-

IMPORT command

Use:

```
IMPORT <filename> /login=<login> /password=<password>
```

Parameters:

<filename> - file to which the settings are to be imported (only binary files are supported).

Examples:

```
avp.com IMPORT settings.dat
```

ADDKEY command

Use:

```
ADDKEY <filename> [/login=<login> /password=<password>]
```

Parameters:

<filename> - name of key file.

Examples:

```
avp.com ADDKEY 00000000.key
```

LICENSE command

Use:

```
LICENSE <command> [/login=<login> /password=<password>]
```

Parameters:

- `command` - command that needs to be executed.
- `/ADD <filename>` - add a key.

- `/ADD <activation code>` - activate the application with an activation code.
- `/DEL` - delete a key.

Examples:

- `avp.com LICENSE /ADD 00000000.key`
- `avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD`
- `avp.com LICENSE /DEL /login=login /password=password`

EXIT command

Use:

```
EXIT /login=<login> /password=<password>
```

Examples:

```
avp.com EXIT /login=login /password=password
```

Error messages

When working with the application, the following error messages may appear:

Table 2. Error messages and return codes

Error message in the command line	Shell return code
Error %d getting thread's context	
Error %d loading QueryInformationThread function	
Error %d opening thread	
Error %d querying thread information	
Error %d suspending thread	
Error in UpdateKSNConfig	
Error in thread safety code: could not acquire a lock	
Error: %S (err 0x%x)	
Error: %S: %s (err 0x%x)	
Error: '%S' has not been completed due to execution timeout	_Shell::_E_TIMEOUT
Error: '%S' is disabled	
Error: Cannot change state for '%S' (%S), task already in state?	SHELL_RET_FAILED
Error: Cannot change state for '%S' (%S), task disabled?	SHELL_RET_FAILED
Error: Cannot create message receiver	
Error: Cannot create task, err=%08X	SHELL_RET_FAILED
Error: Cannot find task '%S'	SHELL_RET_FAILED /SHELL_RET_PARAMETER_INVALID

Error message in the command line	Shell return code
Error: Cannot get product settings	
Error: Cannot get tasks list	SHELL_RET_FAILED
Error: Cannot initialize task parameters block	SHELL_RET_PARAMETER_INVALID
Error: Cannot open configuration file '%S'	
Error: Cannot open list file '%S'	
Error: Cannot set report handler	
Error: Cannot start task '%S', error=%08X	SHELL_RET_NO_LICENCE
Error: Cannot start task '%S', no licence	_Shell::_S_NO_LICENSE
Error: Cannot start task '%S', parameters invalid	SHELL_RET_PARAMETER_INVALID
Error: Cannot verify task parameters block	
Error: Change state failed for task '%S' (%S), error=%08X	SHELL_RET_FAILED
Error: Command unavailable due to password protection disabled	
Error: Configuration file not specified (/C)	
Error: Credential is not obtained, access denied	

Error message in the command line	Shell return code
Error: Duplicate taskid '%S'	
Error: Failed to flush cached data	
Error: File list not specified	
Error: File list not specified (/@)	
Error: Internal error %08X	SHELL_RET_FAILED
Error: Invalid command '%S'	
Error: Invalid parameter '%S'	
Error: Local task control is denied by policy	
Error: NOT IMLEMENTED	SHELL_RET_FAILED
Error: Not enough memory	
Error: Nothing to scan	
Error: Parameter '%S' must contain exclusion specification	
Error: Parameter '%S' must specify size in megabytes	
Error: Parameter not supported by task '%S'	
Error: Password or login is invalid, access denied	
Error: Profile name must be specified	SHELL_RET_PARAMETER_INVALID
Error: Task '%S' not found	SHELL_RET_TASK_FAILED

Error message in the command line	Shell return code
Error: Unknown parameter '%S'	
Error: Usage parameter /APP=<on off>	
Error: Usage parameter /iChecker=<on off>	
Error: Usage parameter /iSwift=<on off>	
Error: cannot open report file %S, error=%d %s	
Error: control of this task is not allowed	
Error: failed to register message handlers	
Error: failed to set INetSwift state	
Error: failed to unregister message handlers	
Error: Local task control is denied by policy	
Scan_Quarantine failed: %	SHELL_RET_FAILED
Scan_Quarantine completed successfully	SHELL_RET_OK
Failed to get AVP_SERVICE_PRODUCT. Error	SHELL_RET_FAILED
Disable command cannot be elevated. Error	SHELL_RET_FAILED

Error message in the command line	Shell return code
Failed to disable product from command line. Error	SHELL_RET_FAILED
Failed to get AVP_SERVICE_PRODUCT. Error	
Failed to get TaskManager service. Error	
Failed to get service locator. Error	
Invalid parameters	SHELL_RET_PARAMETER_INVALID
Failed while activating Global KSN	SHELL_RET_FAILED
Failed to execute command set silent detect. Error	_Shell::_E_FAIL
Failed to execute command silent detect check. Error	_Shell::_E_FAIL
Path not exist	
Cannot write to file, no permission	
Cannot add key file	SHELL_RET_TASK_FAILED
INetSwift state set to	SHELL_RET_OK
Internal error	SHELL_RET_FAILED
Fail to terminate command on user's request	_Shell::_E_BREAK_FAIL
Command is terminated on user's request	_Shell::_E_BREAK_OK

Return codes

Any command executed by the administrator from the command line may result in a return code. Return codes can be general or specific to individual tasks.

The following return codes are available:

- General return codes:
 - 0 - task was completed successfully.
 - 1 - incorrect parameter value.
 - 2 - unknown error.
 - 3 - error during task duration.
 - 4 - the task stopped.
- Return codes of virus scan tasks.
 - 101 - all dangerous objects have been processed.
 - 102 - dangerous objects have been detected.
- Return codes of other tasks:
 - -14 - time out.
 - 239 - error while the task was paused.
 - 240 - task was canceled by the user.
 - -15 - file was blocked by another process and unavailable for processing by the application.
 - -10 - invalid path to object specified.
 - -8 - invalid key.
 - -7 - key has been blacklisted.

- -13 - key is intended for a different product.
- [1-127] - days until license expires.

If more than 127 days remain until license expiration, the return code is 127. If less than 127 days remain until license expiration, the return code equals the actual amount of days. If the license has already expired, the return code is 1.

- 8000045 - insufficient permissions.
- 102 - there are threats that have not been processed.

Table 3. Character-based and numeric values of return codes

Character-based values	Numeric values	Available for commands
_Shell::_E_TIMEOUT	-14	START UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_FAIL	239	UPDATE ROLLBACK SCAN
_Shell::_E_BREAK_OK	240	UPDATE ROLLBACK SCAN
_Shell::_E_FAIL	-3	MESSAGES LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey /Refresh
_Shell::_E_FILE_BLOCKED	-15	UPDATE ROLLBACK SCAN

Character-based values	Numeric values	Available for commands
_Shell::_E_INVALID_PATH	-10	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_INVALID_SYNTAX	-2	UPDATE ROLLBACK MESSAGES SCAN
_Shell::_E_KEY_CORRUPTED	-8	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_KEY_IN_BLST	-7	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
_Shell::_E_KEY_NOT_MATCH	-13	LICENSE: /Add (ActivateByKeyEx) /AddTicket
_Shell::_S_ALL_DETECTION	2	UPDATE ROLLBACK SCAN

Character-based values	Numeric values	Available for commands
_Shell::_S_NO_LICENSE	0	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket /DeleteKey
_Shell::_S_OK	0	UPDATE ROLLBACK SCAN LICENSE: /Add (ActivateByKeyEx) /AddTicket /Refresh
_Shell::_S_PARTIAL_DETECTI ON	3	UPDATE ROLLBACK SCAN
[1-127]	[1-127]	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket

Character-based values	Numeric values	Available for commands
errACCESS_DENIED	8000045	STOP EXITPOLICY

Character-based values	Numeric values	Available for commands
SHELL_RET_FAILED	2	START STOP STATUS STATISTICS MODE HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRE SET SCAN

Character-based values	Numeric values	Available for commands
-SHELL_RET_FAILED	-2	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_NO_LICENCE	2	START UPDATE ROLLBACK SCAN

Character-based values	Numeric values	Available for commands
SHELL_RET_OK	0	START STOP STATUS STATISTICS HELP EXPORT IMPORT EXIT ADDKEY INETSWIFT EXITPOLICY STARTPOLICY UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SLC SPYWARE LETSDUMP MESSAGES RESTORE PBATESTRESET PATCHCOMPATIBILITYRE SET SCAN LICENSE: /Add (ActivateByCode)

Character-based values	Numeric values	Available for commands
SHELL_RET_PARAMETER_INVALID	1	START STOP STATUS STATISTICS EXPORT IMPORT ADDKEY INETSWIFT UPDATE ROLLBACK RENEW DISABLE TRACE\TRACES SPYWARE RESTORE PATCHCOMPATIBILITYRE SET SCAN
-SHELL_RET_PARAMETER_INVALID	-1	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_SCAN_ALL_THREATS	101	UPDATE ROLLBACK SCAN

Character-based values	Numeric values	Available for commands
SHELL_RET_SCAN_NO_THREATS	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_SUSPICIOUS_UNTREATED	0	UPDATE ROLLBACK SCAN
SHELL_RET_SCAN_THREATS	102	UPDATE ROLLBACK SCAN
SHELL_RET_TASK_FAILED	3	STOP EXPORT IMPORT ADDKEY UPDATE ROLLBACK RESTORE SCAN
-SHELL_RET_TASK_FAILED	-3	LICENSE: /Add (ActivateByKey) /Add (ActivateByKeyEx) /AddTicket

Character-based values	Numeric values	Available for commands
SHELL_RET_TASK_STOPPED	4	UPDATE ROLLBACK SCAN

Using task profiles

A *task profile* (also referred to as simply "profile") is a set of settings in text or binary format used for creating a Kaspersky Endpoint Security task.

Profiles are defined in the Windows operating system registry key
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES10SP2\profiles or
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES10SP2\profiles

Profiles have a hierarchical structure. Changes made to the parent profile are also reflected in the profiles within that parent profile. For example, when a parent profile is deleted, all profiles within it are also deleted.

A profile may contain the following settings:

- `flags` – internal mechanism that describes the available operations with the task.
- `enabled` – setting that allows or blocks task startup.
- `installed` – internal mechanism that defines whether modules have been installed for the specific profile.
- `level` – internal mechanism used to distinguish settings by level.
- `type` – text description of the type of task.
- `remote` – setting that enables a task to be run in a separate process.

- `admflags` - settings for managing tasks using Kaspersky Security Center.
- `pid` – ID of the binary module that contains the task implementation.
- `iid` – ID of the task interface defining the class that contains the executable code for the task.
- `persistent` – setting that defines the number of tasks of the same type that can be created in Kaspersky Endpoint Security.
- `idSettings` – ID of the structure of settings.
- `idStatistics` – ID of the structure of task execution statistics.
- `schedule` – task schedule settings.
- `runas` – settings for task run permissions (used only with the parameter value `persistent = 0`).
- `smode` – setting used for postponed task completion.
- `settings` – advanced settings of the task.
- `def` – default task settings.

Kaspersky Endpoint Security performs tasks based on the specified profile settings. When creating a task, the application reads all profiles from the registry and performs the following actions for each profile:

1. Creates an empty structure of settings with the `idSettings` type.
2. Deserializes the values of the `settings` parameter to the prepared structure.

If the `settings` parameter values are not defined, the application uses the values of the `def` parameter and deserializes them to the structure. If there are no values for the `def` parameter, the application uses the default system values for the empty structure of settings.

3. Creates an empty structure with the `idStatistics` type if this parameter was specified in the profile for the created task.
4. Finds a binary module based on the `pid`.
5. Creates an instance of the task based on the `iid` from the binary module.
6. Passes the structure of the settings and statistics to the received instance of the task.
7. If the `installed = 1` and `persistent = 1` parameter values are specified, the application runs the task.
8. If the `persistent = 0` parameter value was specified, the application checks the `schedule` and `smode` parameters and plans the task start based on the specified values.

The Kaspersky Security Center Administration Console lets you create several group tasks of the same type with different settings. For each such task, a profile with the name format `<profile name>${unique id}` is created in the registry. In this format, `unique id` means the unique ID for the task.

Contacting Technical Support

This section describes the ways to get technical support and the terms on which it is available.

In this section:

How to obtain technical support	530
Technical support by phone	530
Technical Support via Kaspersky CompanyAccount	531
Collecting information for Technical Support	532

How to obtain technical support

If you cannot find a solution for your issue in the application documentation or in any of the sources of information about the application (see section "Sources of information about the application" on page [Ошибка! Закладка не определена.](#)), we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Technical support is available only to users who have purchased a commercial license. Users who have received a trial license are not entitled to technical support.

Before contacting Technical Support, please read the support rules (<https://support.kaspersky.com/support/rules>).

You can contact Technical Support in one of the following ways:

- By calling Technical Support by phone (<https://support.kaspersky.com/b2b>) ;
- By sending a request to Kaspersky Lab Technical Support through the Kaspersky CompanyAccount portal (<https://companyaccount.kaspersky.com>).

Technical support by phone

You can call Technical Support representatives from most regions throughout the world. You can find information on ways to receive technical support in your region and contacts for Technical Support on the website of Kaspersky Lab Technical Support (<https://support.kaspersky.com/b2b>).

Before contacting Technical Support, please read the support rules (<https://support.kaspersky.com/support/rules>).

Technical Support via Kaspersky CompanyAccount

Kaspersky CompanyAccount (<https://companyaccount.kaspersky.com>) – is a portal for companies that use Kaspersky Lab applications. The Kaspersky CompanyAccount portal is designed to facilitate interaction between users and Kaspersky Lab experts via electronic requests. You can use Kaspersky CompanyAccount portal to track the status of your electronic requests and store a history of those requests.

You can register all of your organization's employees under a single account on Kaspersky CompanyAccount. A single account lets you centrally manage electronic requests from registered employees to Kaspersky Lab and also manage the privileges of these employees via Kaspersky CompanyAccount.

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 (https://support.kaspersky.com/faq/companyaccount_help).

Collecting information for Technical Support

After you inform Kaspersky Lab Technical Support specialists about your issue, they may ask you to create a *trace file*. The trace file allows you to trace the process of performing application commands step by step and determine the stage of application operation at which an error occurs.

Technical Support specialists may also require additional information about the operating system, processes that are running on the computer, detailed reports on the operation of application components, and application crash dumps.

You can collect the necessary information with the help of Kaspersky Endpoint Security. The collected information can be saved on the hard drive and uploaded later when most convenient for you.

While running diagnostics, Technical Support experts may ask you to change application settings by:

- Activating the functionality that gathers extended diagnostic information.
- Fine-tuning the settings of individual application components, which are not available via standard user interface elements.
- Changing the settings for storage and transmission of diagnostic information that is gathered.
- Configuring the interception and logging of network traffic.

Technical Support experts will provide all the information needed to perform these operations (description of the sequence of steps, settings to be modified, configuration files, scripts, additional command line functionality, debugging modules, special-purpose utilities, etc.) and inform you about the scope of data gathered for purposes of debugging. The extended diagnostic information gathered is saved on the user's computer. Data that has been gathered is not automatically transmitted to Kaspersky Lab.

The settings used to determine the address of the dump server for sending dump files to Kaspersky Lab are stored on the user's computer. If required, the values of these settings can be edited in the operating system registry key

"DumpServerConfigUrl"="https://dmconfig.kaspersky-labs.com/dumpserver/config.xml".

The operations listed above should be performed only under the supervision of Technical Support specialists by following their instructions. Unsupervised changes to application settings performed in ways other than those described in the Administrator's Guide or instructions of Technical Support specialists can slow down or crash the operating system, affect computer security, or compromise the availability and integrity of data being processed.

In this section:

Creating a trace file	533
Contents and storage of trace files	534
Enabling or disabling transmission of dump files and trace files to Kaspersky Lab	537
Sending files to the Technical Support server	537
Enabling and disabling protection of dump files and trace files	538

Creating a trace file

► To create a trace file:

9. Open the main application window.

10. In the main application window, click the button .

The **Support** window opens.

11. In the **Support** window, click the **System tracing** button.

The **Information for Technical Support** window opens.

12. To start the tracing process, select the **Enable tracing** check box.

13. In the **Level** drop-down list, select the trace level.

You are advised to clarify the required trace level with a Technical Support specialist. In the absence of guidance from Technical Support, set the trace level to **Normal (500)**.

14. Reproduce the situation in which the problem occurred.

15. To stop the tracing process, return to the **Information for Technical Support** window and clear the **Enable tracing** check box.

After a trace file is created, you can proceed to uploading tracing results to the Kaspersky Lab server (see section "Sending data files to the Technical Support server" on page [537](#)).

Contents and storage of trace files

The user is personally responsible for ensuring the safety of data collected, particularly for monitoring and restricting access to collected data stored on the computer until it is submitted to Kaspersky Lab.

Trace files are stored on your computer in modified form that cannot be read as long as the application is in use, and are permanently deleted when the application is removed.

Trace files are stored in the ProgramData\Kaspersky Lab folder.

The trace file has the following name format: `KES<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1`.

The Authentication Agent trace file is stored in the System Volume Information folder and has the following name: `KLFD.E.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

You can view data saved in trace files. Please contact Kaspersky Lab Technical Support for advice on how to view data.

All trace files contain the following common data:

- Event time.
- Number of the thread of execution.

The Authentication Agent trace file does not contain this information.

- 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.

Contents of SRV.log, GUI.log, and ALL.log trace files

SRV.log, GUI.log, and ALL.log trace files may store the following information in addition to general data:

- Personal data, including the last name, first name, and middle name, if such data is included in the path to files on the local computer.
- The user name and password if they were transmitted openly. This data can be recorded in trace files during Internet traffic scanning. Traffic is recorded in trace files only from trafmon2.ppl.
- The user name and password if they are contained in HTTP headers.
- The name of the Microsoft Windows account if the account name is included in a file name.
- Your email address or a web address containing the name of your account and password if they are contained in the name of the object detected.
- Websites that you visit and redirects from these websites. This data is written to trace files when the application scans websites.
- Proxy server address, computer name, port, IP address, and user name used to sign in to the proxy server. This data is written to trace files if the application uses a proxy server.
- Remote IP addresses to which your computer established connections.
- Message subject, ID, sender's name and address of the message sender's web page on a social network. This data is written to trace files if the Web Control component is enabled.

Contents of HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log trace files

In addition to general data, the HST.log trace file contains information about the execution of a database and application module update task.

In addition to general data, the BL.log trace file contains information about events occurring during operation of the application, as well as data required to troubleshoot application errors. This file is created if the application is started with the avp.exe –bl parameter.

In addition to general data, the Dumpwriter.log trace file contains service information required for troubleshooting errors that occur when the application dump file is written.

In addition to general data, the WD.log trace file contains information about events occurring during operation of the avpsus service, including application module update events.

In addition to general data, the AVPCon.dll.log trace file contains information about events occurring during the operation of the Kaspersky Security Center connectivity module.

Contents of trace files of application plug-ins

Trace files of application plug-ins contain the following information in addition to general data:

- The shellex.dll.log trace file of the plug-in that starts the scan task from the context menu contains information about the execution of the scan task and data required to debug the plug-in.
- The mcou.OUTLOOK.EXE trace file of the Mail Anti-Virus plug-in may contain parts of email messages, including email addresses.

Contents of the Authentication Agent trace file

In addition to general data, the Authentication Agent trace file contains information about the operation of Authentication Agent and the actions performed by the user with Authentication Agent.

Enabling or disabling transmission of dump files and trace files to Kaspersky Lab

► *To enable or disable transmission of dump files and trace files to Kaspersky Lab:*

16. From the application settings window in the left part of the window, select the **Advanced Settings** section.

Advanced application settings are displayed in the right part of the window.

17. In the **Operating mode** section, click the **Settings** button.

The **Operating mode** window opens.

18. In the **Operating mode** window, select the **Enable dump writing** check box to enable the application to write application dump files.

19. Do one of the following:

- Select the **Send dump and trace files to Kaspersky Lab** check box if you want the application to show a prompt in the **Upload information for Technical Support to server** window to send dump and trace files to Kaspersky Lab for analysis of the causes of the application failure at the next startup of the application.
- Otherwise, clear the **Send dump and trace files to Kaspersky Lab** check box.

20. Click **OK** in the **Operating mode** window.

21. To save the changes, click the **Save** button in the main application window.

Sending files to the Technical Support server

Files containing information about the operating system, trace files, and dump files must be sent to Kaspersky Lab Technical Support experts.

► *To send files to the Technical Support server:*

22. Restart Kaspersky Endpoint Security after any malfunction in its operation.

This opens the **Previous application startup failed** window.

The **Previous application startup failed** window will open each time Kaspersky Endpoint Security is started (including after restarting the computer) until you send the dump files or trace files to Technical Support or until you click the **Do not send** button.

23. In the **Previous application startup failed** window, open the list of generated files by clicking **here**.

24. Select the check boxes next to those files that you want to send to Technical Support.

25. Click the **Show Statement text** button.

The **Data Provision Statement** window opens.

26. Read the text of the Data Provision Statement and click the **Close** button.

27. In the **Previous application startup failed** window, select the **I agree with the Data Provision Statement** check box.

28. Click the **Send** button.

This opens the **Request number** window.

29. In the **Request number** window, specify the number that was assigned to your request when you contacted Technical Support through Kaspersky CompanyAccount.

30. Click **OK**.

The selected data files are packed and sent to the Technical Support server.

Enabling and disabling protection of dump files and trace files

Dump files and traces contain information about the operating system, as well as confidential data of the user (see "Contents and storage of trace files on page [534](#)). To prevent unauthorized access to such data, you can enable protection of dump files and trace files.

If protection of dump files and trace files is enabled, the files can be accessed by the following users:

- Dump files can be accessed by the system administrator and local administrator, and by the user that enabled the writing of dump files and trace files.
- Trace files can be accessed only by the system administrator and local administrator.

► *To enable or disable protection of dump files and trace files:*

31. From the application settings window select the **Advanced Settings** section on the left.

The application settings are displayed in the right part of the window.

32. In the **Operating mode** section, click the **Settings** button.

The **Operating mode** window opens.

33. Do one of the following:

- Select the **Enable dump and trace files protection** check box if you want to enable protection.
- Clear the **Enable dump and trace files protection** check box if you want to disable protection.

34. Click **OK** in the **Operating mode** window.

35. To save the changes, click the **Save** button in the main application window.

Dump files and trace files that were written while protection was active remain protected even after this function is disabled.