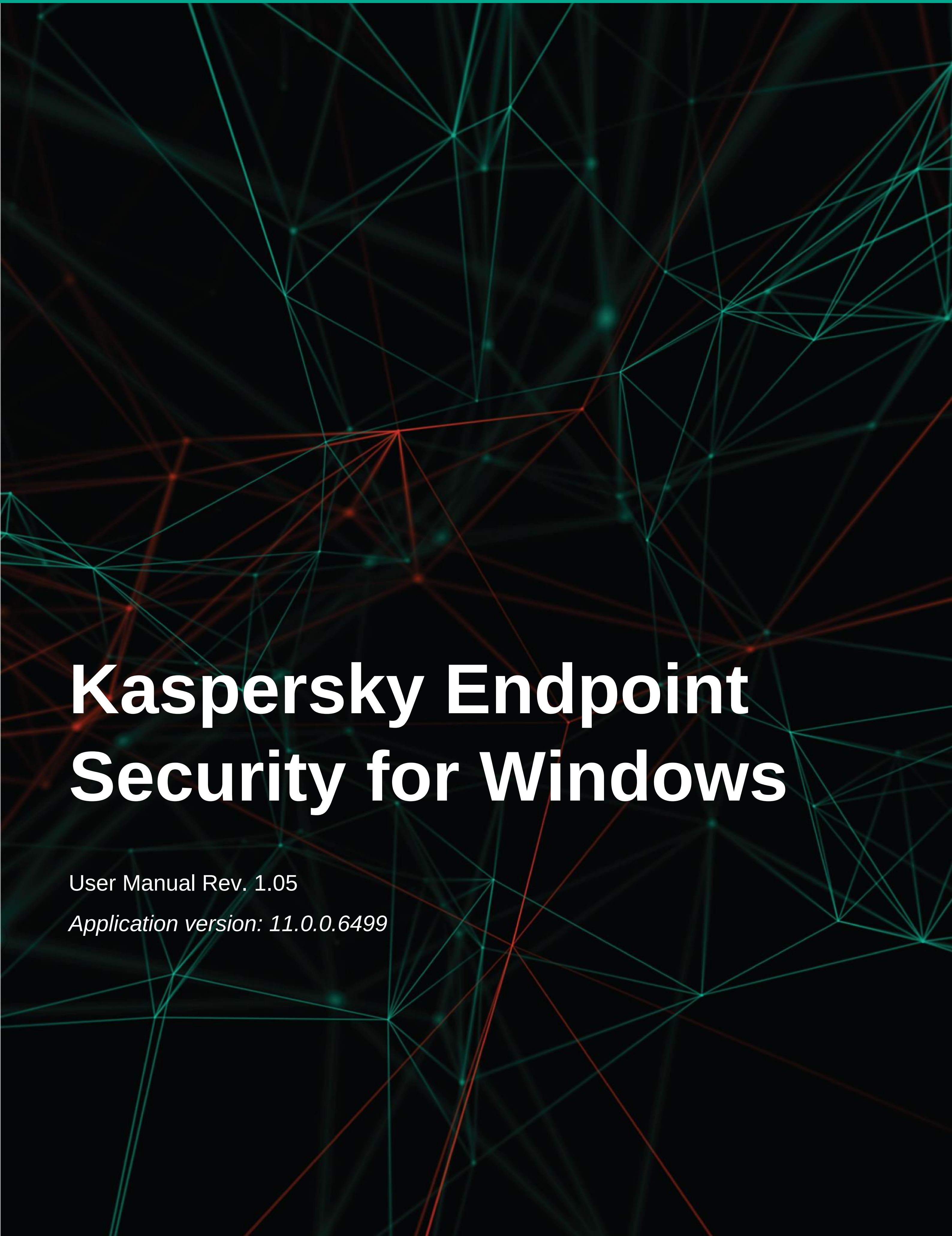


Kaspersky Endpoint Security for Windows

User Manual Rev. 1.05

Application version: 11.0.0.6499

Table of contents

About Kaspersky Endpoint Security for Windows

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

In this section:

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 file ksn_<language ID>.txt, in which you can read through the terms of participation in Kaspersky Security Network (see section "Participation in Kaspersky Security Network" on page 12).
- The license.txt file, which you can use to view the End User License Agreement and the Privacy Policy.
- 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
- Intel Pentium 1 GHz processor (or compatible equivalent)
- RAM:
  - For a 32-bit operating system - 1 GB
  - For a 64-bit operating system - 2 GB

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/kes11 http://support.kaspersky.com/kes11.

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/kes11 http://support.kaspersky.com/kes11.

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 behavior of authorized users

Authorized 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 authorized 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. Unauthorized individuals shall not get the password of an authorized 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 window" on page 357).

The administrator performs installation, configuration and administration of Kaspersky Endpoint Security locally 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.

If a client computer with Kaspersky Endpoint Security installed is running under a Kaspersky Security Center policy, the administrator can restrict availability of operations or managing operations with the application. In this case, the application will prompt the user for the password (see section "Password protection window" on page 357) when the user attempts to perform a protected operation in the Kaspersky Endpoint Security local interface.

Application functionality after license expiration

Administrators should maintain active license (see section "Key addition group task settings section" on page 363) for Kaspersky Endpoint for Windows at all times to ensure lasting data protection.

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

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.
  - **Product 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

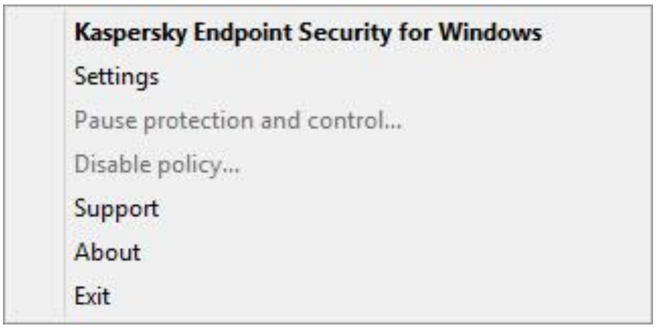
The context menu of the application icon contains the following items:

- **Kaspersky Endpoint Security for Windows**. Opens the main application window. In this window, you can adjust the operation of application components and tasks, and view the statistics of processed files and detected threats.
- Settings Opens the **Settings** 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.

  > Kaspersky Security Network is used by Kaspersky Endpoint Security regardless of whether the operation of protection and control components is paused / resumed.

- **Disable policy** / **Enable policy**. Disables / enables the Kaspersky Security Center policy. This context menu item is available if a policy has been applied to a computer on which Kaspersky Endpoint Security is installed, 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.



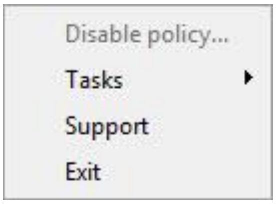
Kaspersky Endpoint Security for Windows
Settings
Pause protection and control...
Disable policy...
Support
About
Exit

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

Simplified application interface

If a Kaspersky Security Center policy configured to display the simplified application interface is applied to a client computer on which Kaspersky Endpoint Security is installed, the main application window is not available on this client computer. Right-click to open the context menu of the Kaspersky Endpoint Security icon (see the figure below) containing the following items:

- **Disable policy**. Disables the Kaspersky Security Center policy on the client computer that has Kaspersky Endpoint Security installed. This context menu item is available if a policy has been applied to the computer and a password for disabling the Kaspersky Security Center policy has been set.
- Tasks Drop-down list containing the following items:
  - Updater
  - Rollback
  - **Full Scan**.
  - **Custom Scan**.
  - **Critical Areas Scan**.
  - **Integrity Check**.
- **Support**. This opens the **Support** window containing information necessary for contacting Kaspersky Lab Technical Support.
- **Exit**. Version of Kaspersky Endpoint Security.



Disable policy...
Tasks
Support
Exit

Main application window

Kaspersky Endpoint Security for Windows

Clicking the **Kaspersky Endpoint Security for Windows** link opens the **About** window. This window lets you view the application version number.

Button ?

Clicking the button opens the Help system section of Kaspersky Endpoint Security.

Threat detection technologies

Section in the upper part of the application window containing the following information:

- The left part of the section displays a list of threat detection technologies. The number of threats that were detected using the specific technology appears to the right of the name of each threat detection technology. The following technologies are included in the list of threat detection technologies:
  - **Machine learning**. Threat detection technology that employs mathematical machine learning models to make autonomous decisions on the extent to which an object is malicious.
  - **Cloud analysis**. Threat detection technology in which Kaspersky Endpoint Security uses cloud databases for threat detection.
  - **Expert analysis**. Threat detection technology in which threat detection is performed with the involvement of Kaspersky Lab information security experts.
  - **Behavior analysis**. Technology in which Kaspersky Endpoint Security analyzes application activity and blocks any malicious activity.
  - **Automatic analysis**. Threat detection technology in which threat detection is performed using automatically generated templates.
- Depending on the presence of active threats, the center of the section displays one of the following captions:
  - **No threats**. If this caption is displayed, clicking the **Threat detection technologies** section opens the **Threat detection technologies** window, which provides a brief description of the threat detection technologies as well as the status and global statistics of the Kaspersky Security Network cloud service infrastructure.
  - **N active threats**. If this caption is displayed, clicking the **Threat detection technologies** section opens the **Active threats** window, which displays a list of events associated with infected files that were not processed for some reason.

Protection components

Clicking this button opens the **Protection components** window. In this window, you can view the operating status of installed components. From this window, you can also open a subsection in the **Settings** window containing the settings of any installed component except encryption components.

Tasks

Clicking this button opens the **Tasks** window. In this window, you can manage Kaspersky Endpoint Security tasks that are used to update application modules and databases, scan for viruses and other malware, and run an integrity check on application modules.

Reports

Clicking this button opens the **Reports** window. This window lets you view reports on the overall operation of Kaspersky Endpoint Security and on the performance of individual application components, scan tasks, update tasks, and integrity check tasks.

Backup

Clicking this button opens the **Backup** tab in the **Repositories** window. On this tab, you can view a list of files that Kaspersky Endpoint Security changed during the disinfection process or deleted. In this storage, files are stored in a special format and cannot pose a threat.

Support

Clicking this button opens the **Support** window. You can view the following details in this window:

- Kaspersky Endpoint Security version.
- Databases and application modules release date and time.
- Operating system version.
- Key (if the application is activated).

You can perform the following actions by using the buttons in the lower part of the window:

- Enable system tracing.
- Go to the Knowledge Base page of Technical Support.
- Visit the user forum.
- Go to the page of the Kaspersky CompanyAccount portal.
- Start the process of restoring access to an encrypted device.

These buttons are displayed by default. If a Kaspersky Security Center policy has been applied to the computer, the administrator can specify other links to web resources to be displayed in the **Support** window.

Settings

Clicking this button opens the **Settings** window. In this window, you can configure the application settings. After installation of the application and for all components added after application installation, all settings take the default settings.

Button ✉ / ✉ / ✉

Clicking this button opens the **Events** window. This window lets you view information about the available updates as well as requests for access to encrypted files and devices.

The button is available only when there are requests for access or uninstalled updates.

The button color can change depending on the importance and novelty of notifications:

- ✉ - there are no unread notifications.
- ✉ - there are unread notifications.
- ✉ - there are critically important unread notifications.

License

Clicking the **License** link opens the **Licensing** window. This window lets you view information about the current license as well as activate the application or purchase a license.

On the left of the **License** link is one of the following icons:

- 🏅 – the application is activated.
- 🏅 – the application has not been activated or the license has expired.

Protection components window

In the **Protection components** window, you can view a list of installed Kaspersky Endpoint Security components that are grouped into the following sections:

- **Essential Threat Protection**.
- **Advanced Threat Protection**.
- **Security Controls**.
- **Data Encryption**.

Each component in the **Essential Threat Protection**, **Advanced Threat Protection** and **Security Controls** sections is characterized by one of the following icons located to the left of the component names:

- The ✓ icon represents the *Enabled* status.
- The ⏸ icon represents the *Paused* status.
- The ✗ icon represents the *Malfunctioned* status.
- The ⊗ icon represents the *Disabled* status.

By clicking any of the components in the **Essential Threat Protection**, **Advanced Threat Protection** or **Security Controls** section, you can open the subsection in the **Settings** window containing the settings of this component.

Each component in the **Data Encryption** section is characterized by one of the following icons located to the left of the component names:

- The ✓ icon represents the *Encryption settings applied* status. This icon is displayed if the encryption component has been installed and the Kaspersky Security Center policy with configured encryption settings is active.
- The ⊗ icon represents the *Encryption settings not applied* status. This icon appears when the encryption component is installed but the Kaspersky Security Center policy is inactive or the encryption settings are not configured in it.
- The ⏸ icon represents the *Encryption functionality is unavailable* status. This icon is displayed in one of the following cases:
  - The Kaspersky Endpoint Security application is not activated.
  - The Kaspersky Endpoint Security license has expired.
  - The Kaspersky Endpoint Security license does not support encryption.
- The ✗ icon represents the *Component malfunctioned* status. This icon is displayed if an error occurred in the operation of the encryption component.

Application activity monitor

Click the **Application activity monitor** link to open the **Application activity monitor** tab of the **Host Intrusion Prevention** window. This tab lets you view a summary of the activity of applications that are running in the operating system.

Network Monitor

Click the **Network Monitor** link to open the **Network activity** tab of the **Network Monitor** window, which displays all currently active network connections with the user's computer.

Tasks window

In the **Tasks** window, you can manage the operation of Kaspersky Endpoint Security tasks that are used to update application modules and databases, scan files for viruses and other malware, and run an integrity check. In this window you can manage the operation of Kaspersky Endpoint Security tasks created on the Kaspersky Security Center Administration Server by the administrator.

This window displays the following items:

- Task name
- Task status The following task statuses are possible:
  - *Manually*.
  - *Automatically*.
  - *<Date and time of next scheduled run>*.
  - *Running*.
  - *Stopped*.
  - *Never started*.
  - *Failed*.
  - *Unknown*.
- Statistics and progress status of a task that is running or has been stopped (the *Running* or *Stopped* status). The statistics are shown on the right of the task status, and also in the line following the task status line.
- Statistics of the last instance of a task that has been completed (the *Manually*, *<Date and time of next scheduled run>*, or *Automatically* status). The statistics are shown in the line following the task status line.
- Error description, if the task completes with an error (the *Failed* status). The statistics are shown in the line following the task status line.

Start / Stop

Button located under the task information. By clicking this button, you can start / stop this task.

Settings

Button located under the task information. By clicking this button, you can open the subsection in the **Settings** window containing the settings of this task.

Reports

Button located under the task information. By clicking this button, you can open a report on events that occurred when running this task.

Participation in Kaspersky Security Network

This section contains information about participation in Kaspersky Security Network and instructions on how to enable or disable use of Kaspersky Security Network.

In this section:

Kaspersky Security Network is not available.

About participation in Kaspersky Security Network

To protect your computer more effectively, Kaspersky Endpoint Security uses data that is gathered from users around the globe. *Kaspersky Security Network* is designed to collect such data.

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to the online Kaspersky Lab Knowledge Base that contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Endpoint Security to new threats, improves the performance of some protection components, and reduces the likelihood of false positives.

Depending on the location of the infrastructure, there is a Global KSN service (the infrastructure is hosted by Kaspersky Lab servers) and a Private KSN service.

Thanks to users who participate in KSN, Kaspersky Lab is able to promptly gather information about types and sources of threats, develop solutions for neutralizing them, and minimize the number of false alarms displayed by application components.

When using extended KSN mode, the application automatically sends its resultant operating statistics to KSN. The application can also send certain files (or parts of files) that hackers could use to harm the computer or data to Kaspersky Lab for additional scanning.

> For more detailed information about sending Kaspersky Lab statistical information that is generated during participation in KSN, and about the storage and destruction of such information, please refer to the Kaspersky Security Network Statement and the Kaspersky Lab website. (https://www.kaspersky.com/products-and-services-privacy-policy).https://www.kaspersky.com/products-and-services-privacy-policy The ksn_en.txt file containing the text of the Kaspersky Security Network Statement is included in the application distribution kit.
> To reduce the load on KSN servers, Kaspersky Lab may release application anti-virus databases that temporarily disable or partly restrict requests to Kaspersky Security Network. In this case, the status of the connection to KSN appears as *Enabled with restrictions*.

User computers managed by Kaspersky Security Center Administration Server can interact with KSN via the KSN Proxy service.

The KSN Proxy service provides the following capabilities:

- The user's computer can query KSN and submit information to KSN even without direct access to the Internet.
- KSN Proxy caches processed data, thereby reducing the load on the external network connection and speeding up receipt of the information that is requested by the user's computer.

More details about the KSN Proxy service can be found in the Kaspersky Security Center Help Guide.

KSN Proxy settings can be configured in the properties of policies *of Kaspersky Security Center* (see section "*Managing policies*" on page 166).

Use of Kaspersky Security Network is voluntary. The application prompts you to use KSN during initial configuration of the application. Users can begin or discontinue participation in KSN at any time.

Kaspersky Security Network is not available.

Kaspersky Security Network subsection

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.

The check box remains selected or cleared depending on what was chosen during the initial configuration of Kaspersky Endpoint Security

KSN Statement

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.

Enable extended KSN mode

The check box enables / disables extended Kaspersky Security Network (KSN) mode in the operation of Kaspersky Endpoint Security. The use of KSN is voluntary.

If the check box is selected, Kaspersky Endpoint Security sends its operation statistics to the KSN server and can send to Kaspersky Lab for additional analysis any files (or parts of files) that can be used by intruders to harm the computer or data.

If the check box is cleared, Kaspersky Endpoint Security uses basic KSN functions.

The check box remains selected or cleared depending on what was chosen during the initial configuration of Kaspersky Endpoint Security

KSN network

Information on the type of KSN network used by the application: **Global KSN** or **Private KSN**.

Enable cloud mode for protection components

This check box enables or disables cloud mode for protection components.

If the check box is selected, Kaspersky Endpoint Security uses the light version of anti-virus databases, which reduces the load on operating system resources.

Kaspersky Endpoint Security downloads the light version of anti-virus databases during the next update after the check box was selected.

If the check box is cleared, Kaspersky Endpoint Security uses the full version of anti-virus databases.

Kaspersky Endpoint Security downloads the full version of anti-virus databases during the next update after the check box was cleared.

This check box is available if the **Enable Kaspersky Security Network** check box is selected.

This check box is selected by default.

Behavior Detection

This section contains information about Behavior Detection and instructions on how to configure the component settings.

In this section:

About Behavior Detection

The Behavior Detection component collects data on the actions of applications on your computer and provides this information to other protection components to improve their performance.

The Behavior Detection component utilizes Behavior Stream Signatures (BSS) for applications. These signatures contain sequences of actions that Kaspersky Endpoint Security classifies as dangerous. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the selected responsive action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

Behavior Detection subsection

Enable Behavior Detection

This check box enables / disables the Behavior Detection component.

If the check box is selected, Kaspersky Endpoint Security monitors the activity of applications in the system and provides information about the activity of these applications to other components for more effective protection.

If the check box is cleared, Kaspersky Endpoint Security does not monitor the activity of applications in the system.

This check box is selected by default.

On detecting malware activity

The items in this drop-down list determine the possible actions taken by Kaspersky Endpoint Security when it detects malicious activity:

- **Delete file**. If this item is selected, on detecting malicious activity Kaspersky Endpoint Security deletes the executable file of the malicious application and creates a backup copy of the file in Backup.
- **Terminate the program**. If this item is selected, on detecting malicious activity Kaspersky Endpoint Security terminates this application.
- **Inform**. If this item is selected and malware activity of an application is detected, Kaspersky Endpoint Security adds information about the malware activity of the application to the list of active threats.

The **Delete file** option is selected by default.

In the **Protection of shared folders against external encryption** section you can configure the settings for operations performed from a remote computer.

Enable protection of shared folders against external encryption

The check box enables or disables protection of shared folders against external encryption.

If the check box is selected, Kaspersky Endpoint Security monitors the following operations performed from a remote computer:

- Deletion of a file
- Modification of file contents
- Modification of file size
- Movement of a file.

If the check box is cleared, Kaspersky Endpoint Security does not monitor the following operations performed from a remote computer.

This check box is cleared by default.

On detection of external encryption of shared folders

The items in this drop-down list determine the possible actions taken by Kaspersky Endpoint Security when it detects attempts to encrypt shared folders from a remote computer:

- **Block connection**. If this item is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security blocks network activity originating from the computer attempting to modify files and creates backup copies of modified files.

> If the Remediation Engine component is enabled and the **Block connection** option is selected, Kaspersky Endpoint Security restores modified files from backup copies.

- **Inform**. If this item is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security adds information about this attempt to modify files in shared folders to the list of active threats.

> Kaspersky Endpoint Security prevents external encryption of only those files that are located on media that have the NTFS file system and are not encrypted by the EFS system.

The **Block connection** option is selected by default.

Block connection for

The time for which Kaspersky Endpoint Security blocks the network activity of the remote computer performing encryption of shared folders.

The default value is 60 minutes.

Exclusions

The Audit Logon service must be enabled to enable the list of computers excluded from protection of shared folders against external encryption. By default, the Audit Logon service is disabled (for detailed information about enabling the Audit Logon service, please visit the Microsoft website).

Clicking the button opens the **Exclusions** window. This window lets you create a list of IP addresses of remote computers from which attempts to modify files in shared folders will not be monitored.

Exclusions window

The Audit Logon service must be enabled to enable the list of computers excluded from protection of shared folders against external encryption. By default, the Audit Logon service is disabled (for detailed information about enabling the Audit Logon service, please visit the Microsoft website).

Add

Clicking this button opens the **Computers** window. This window lets you add the IP address or name of a computer to the list of exclusions.

Edit

Clicking this button opens the **Computers** window. In this window, you can edit the IP address or name of a computer in the list of exclusions.

This button is available if an item is selected in the list of exclusions.

Delete

Clicking this button causes Kaspersky Endpoint Security to remove the selected item from the list of exclusions.

The button is available if you have selected any item in the list of exclusions.

Computers

List of computers from which attempts to encrypt shared folders will not be monitored.

Computers window

Field for entering the name or IP address of the computer.

Exploit Prevention

This section contains information about Exploit Prevention and instructions on how to configure the component settings.

In this section:

About Exploit Prevention

The Exploit Prevention component tracks executable files that are run by vulnerable applications. When there is an attempt to run an executable file from a vulnerable application that was not performed by the user, Kaspersky Endpoint Security blocks this file from running. Information about the blocked launch of the executable file is stored in the Exploit Prevention report.

Exploit Prevention subsection

Enable Exploit Prevention

This check box enables / disables the Exploit Prevention component.

If the check box is selected, Kaspersky Endpoint Security keeps track of executable files launched by vulnerable applications.

If the check box is deselected, Kaspersky Endpoint Security does not keep track of executable files launched by vulnerable applications.

This check box is selected by default.

On detecting exploit

The items in this drop-down list determine the possible actions taken by Kaspersky Endpoint Security on detection of an exploit:

- **Block operation**. If this item is selected, on detection of an exploit Kaspersky Endpoint Security blocks all operations attempted by the exploit.
- **Inform**. If this item is selected and an exploit is detected, Kaspersky Endpoint Security adds information about this exploit to the list of active threats.

The **Block operation** option is selected by default.

Enable system process memory protection

This check box enables / disables protection of system process memory.

If this check box is selected, Kaspersky Endpoint Security blocks external processes that attempt to access system process memory.

If this check box is cleared, Kaspersky Endpoint Security does not block external processes that attempt to access system process memory.

This check box is selected by default.

Host Intrusion Prevention

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 5).

This section contains information about Host Intrusion Prevention and instructions on how to configure the component settings.

In this section:

About Host Intrusion Prevention

The Host Intrusion Prevention component prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources and personal 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 privilege 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, the Host Intrusion Prevention component checks the security of the application and places it into one of the trust groups. A trust group defines the rules that Kaspersky Endpoint Security applies when controlling application activity.

You are advised to participate in Kaspersky Security Network to improve the performance of the Host Intrusion Prevention component (see section "Participation in Kaspersky Security Network" on page 12). Data that is obtained through Kaspersky Security Network allows you to sort applications into groups with more accuracy and to apply optimum application privilege control rules.

The next time the application starts, Host Intrusion Prevention verifies the integrity of the application. If the application is unchanged, the component applies the current application privilege control rules to it. If the application has been modified, Host Intrusion Prevention analyzes the application as if it were being started for the first time.

Host Intrusion Prevention subsection

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

- Enable and disable Host Intrusion Prevention.
- Configure rules for applications and protected resources.
- Configure the settings for assigning applications to trust groups.

The following settings are available:

Enable Host Intrusion Prevention

This check box enables or disables the operation of the Host Intrusion Prevention component.

If the check box is selected, the Host Intrusion Prevention component starts at Kaspersky Endpoint Security startup and registers the activity of applications in the system.

If the check box is cleared, the Host Intrusion Prevention component is disabled.

This check box is selected by default.

Applications

Clicking this button opens the **Application privilege control** tab in the **Host Intrusion Prevention** window. This tab shows the list of applications, access to which is monitored by the Host Intrusion Prevention component. Applications are assigned to trust groups.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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 **Host Intrusion Prevention** window. On this tab, you can view the list of personal data and operating system settings and resources to which the Host Intrusion Prevention component controls access. You can also enable the protection of any resources in the list or add other resources to the list.

Update control rules for previously unknown applications from KSN databases

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

If the check box is selected, the Host Intrusion Prevention component updates the application privilege 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, the Host Intrusion Prevention component places digitally signed applications in the Trusted group.

If this check box is cleared, the Host Intrusion Prevention component 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.

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

This check box enables / disables the option to automatically delete application privilege 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 the Host Intrusion Prevention component deletes the application privilege control rules of applications that have not been started for more than 60 days.

If trust group cannot be defined, automatically move applications to

Items in this drop-down list determine to which trust group Kaspersky Endpoint Security will assign an unknown application.

You can choose one of the following items:

- **Low Restricted**.
- **High Restricted**.
- **Untrusted**.

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 privilege control 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

Table of application privilege control rules for applications that are categorized into trust groups. Kaspersky Endpoint Security applies the application privilege control rules to regulate applications' access to operating system processes and resources.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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 privilege 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 applications 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 Host Intrusion Prevention and File Threat Protection 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 the Host Intrusion Prevention component 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 **Configure application privilege 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.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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.

Geographic spread

Popularity of the application among Kaspersky Security Network participants by country.

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 ⊞ and ⊟ 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 or disables the scan exclusion for all files opened by the specific application.

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 or disables monitoring of the file- and network activity of an application in the operating system by the Host Intrusion Prevention, Behavior Detection, Exploit Prevention, Remediation Engine 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 or disables the scan exclusion for network traffic generated by the specific application.

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 scan exclusion settings for network traffic.

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 the Host Intrusion Prevention component 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.

/Refresh

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. The Host Intrusion Prevention component 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, the Host Intrusion Prevention component protects the resource.

If the check box next to a resource is cleared, the Host Intrusion Prevention component 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, in addition to 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 the resources that the user has excluded from the protection scope of the Host Intrusion Prevention component. 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, the Host Intrusion Prevention component does not control access to this resource.

If the check box next to a resource is cleared, the Host Intrusion Prevention component 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 must be protected by Application 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\* – 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 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` key 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 must be protected by the Host Intrusion Prevention component.

The Host Intrusion Prevention component 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.
- ProcMon 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.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 user has placed applications in the Untrusted group.

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

- **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.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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.

Remediation Engine

This section contains information about Remediation Engine and instructions on enabling or disabling the component.

In this section:

About Remediation Engine

The Remediation Engine lets Kaspersky Endpoint Security roll back actions that have been performed by malware in the operating system.

When rolling back malware activity in the operating system, Kaspersky Endpoint Security handles the following types of malware activity:

- File activity.

  Kaspersky Endpoint Security deletes executable files that have been created by a malicious program and are located on any media, except for network ones.

  Kaspersky Endpoint Security deletes executable files that were created by programs that have been infiltrated by malware.

  Kaspersky Endpoint Security does not restore changed or deleted files.

- Registry activity.

  Kaspersky Endpoint Security deletes partitions and registry keys that have been created by malware.

  Kaspersky Endpoint Security does not restore modified or deleted partitions and registry keys.

- System activity.

  Kaspersky Endpoint Security terminates processes that have been initiated by a malicious program.

  Kaspersky Endpoint Security terminates processes into which a malicious program has penetrated.

  Kaspersky Endpoint Security does not resume processes that have been halted by a malicious program.

- Network activity.

  Kaspersky Endpoint Security blocks the network activity of malicious programs.

  Kaspersky Endpoint Security blocks network activity of processes into which a malicious program has penetrated.

A rollback of malware actions can be started by the File Threat Protection (see page 49) component or during a virus scan.

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.

Remediation Engine subsection

Enable Remediation Engine

This check box enables / disables the Remediation Engine component.

If the check box is selected, when Kaspersky Endpoint Security detects malicious applications it rolls back the actions of these applications in the operating system.

If the check box is cleared, Kaspersky Endpoint Security does not roll back the actions of these applications in the operating system.

This check box is selected by default.

File Threat Protection

This section contains information about the File Threat Protection component and instructions on how to configure the component settings.

In this section:

About File Threat Protection

The File Threat Protection component lets you prevent infection of the file system of the computer. By default, the File Threat Protection component starts together with Kaspersky Endpoint Security, continuously resides in the computer's RAM, and scans files that are opened or run on the computer and on its attached drives to find viruses and other potential threats. The scan is performed according to the application settings.

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. 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 Threat Protection component settings.

File Threat Protection subsection

Enable File Threat Protection

This check box enables or disables the File Threat Protection component.

If the check box is selected, the File Threat Protection component 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, the File Threat Protection component is configured with the settings that are recommended by Kaspersky Lab experts.

If the check box is cleared, File Threat Protection 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, the File Threat Protection component takes the strictest control of all files that are opened, saved, and started. The File Threat Protection component scans all file types on all hard drives, removable drives, and network drives 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. The File Threat Protection component scans only the specified file formats on all hard drives, removable drives, and network drives of the computer, and embedded OLE objects. The File Threat Protection component 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. The File Threat Protection component scans only files with specified extensions on all hard drives, removable drives, and network drives of the computer. The File Threat Protection component does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

Clicking this button opens the **File Threat Protection** 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 the File Threat Protection component performs if infected files are detected when scanning.

> Before attempting to disinfect or delete an infected file, the File Threat Protection component creates a backup copy in case it becomes necessary to restore the file or it becomes possible to disinfect the file at a later time.

Disinfect, delete if disinfection fails

If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component deletes these files.

This option is selected by default.

Disinfect, block if disinfection fails

If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component blocks these files.

Block

If this option is selected, the File Threat Protection component automatically blocks all infected files without attempting to disinfect them.

General tab

The **File types** section allows you to select the types of files that the File Threat Protection component scans.

> The File Threat Protection component assumes that files without an extension are executable files. The File Threat Protection component always scans executable files, regardless of the file types that are selected for scanning.

All files

If this setting is selected, the File Threat Protection component scans all files without exception (all formats and extensions).

Files scanned by format

If this setting is selected, the File Threat Protection component scans infectable files only. 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, the File Threat Protection component scans infectable files only. 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 the File Threat Protection component.

The **Protection scope** section allows you to create a list of objects that are scanned by the File Threat Protection component.

Protection scope

Contains objects that are scanned by the File Threat Protection component. A scan object may be a hard drive or network drive, folder, file, or file name mask.

By default, the File Threat Protection component scans files that are started on any hard drives, removable drives, or network 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, the File Threat Protection component scans it.

If the check box next to the name of a scan object is cleared, the File Threat Protection component 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 the File Threat Protection component.

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

Clicking 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 Threat Protection** 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, the File Threat Protection component 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.

The File Threat Protection component 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 the File Threat Protection component uses when scanning the computer.

Machine learning and signature analysis

The machine learning and signature analysis method uses the Kaspersky Endpoint Security databases that contain descriptions of known threats and ways to neutralize them. Protection that uses this method provides the minimum acceptable security level.

Based on the recommendations of Kaspersky Lab experts, machine learning and signature analysis 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 heuristic analysis level. The heuristic analysis level ensures a 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 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 heuristic analysis level, the probability of detecting threats is lower than at the **medium scan** and **deep scan** heuristic analysis levels. Scanning is faster and less resource-intensive.

  The **Light scan** heuristic analysis level is selected 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** levels of heuristic analysis. At this heuristic analysis level, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels of heuristic analysis. 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. The File Threat Protection component scans both simple 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 the File Threat Protection component scans for viruses and other 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**. The File Threat Protection component scans all archives.
- **New**. The File Threat Protection component scans only new archives that have been modified since the last scan.

  The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables or disables scanning of distribution packages.

This check box is cleared by default.

The following scan options are available:

- **All**. The File Threat Protection component scans all distribution packages.
- **New**. The File Threat Protection component scans only new distribution packages that have been modified 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 or disables the function that the File Threat Protection component 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**. The File Threat Protection component scans all files in office formats.
- **New**. The File Threat Protection component scans only new Office format files that have been modified since the last 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.

Unpack 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 the File Threat Protection component.

Smart mode

In this scan mode, the File Threat Protection component 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, the File Threat Protection component 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, the File Threat Protection component 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, the File Threat Protection component 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 run the files.

The **Scan technologies** section contains scan technologies that the File Threat Protection component 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 the File Threat Protection component.

By schedule

The check box enables or disables the function that lets you pause the File Threat Protection component for a specified amount of 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 the File Threat Protection component is paused.

The button is available if the **By schedule** check box is selected.

At application startup

This check box enables or disables the function that pauses the File Threat Protection component while the user works with applications that require significant resources of 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 require the File Threat Protection component to be paused 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 the File Threat Protection component.

The following settings are available:

Pause task at

Field for entering the time at which the File Threat Protection component is paused. The time is specified in HH:MM format.

Resume task at

Field for entering the time at which the File Threat Protection component is resumed. 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 the File Threat Protection component to terminate its operation.

The following settings are available:

Applications

This list includes applications during whose operation Kaspersky Endpoint Security pauses the operation of the File Threat Protection component. 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 the File Threat Protection component 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.

Web Threat Protection

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 5).

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

In this section:

About Web Threat Protection

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.

The Web Threat Protection component 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.

The Web Threat Protection component intercepts every web page or file that is accessed by the user or an application via the HTTP or FTP protocol and analyzes them for viruses and other threats. 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 Threat Protection component settings.

Web Threat Protection subsection

Enable Web Threat Protection

This check box enables or disables the Web Threat Protection component.

If the check box is selected, the Web Threat Protection component protects information that arrives on the computer over the HTTP and FTP protocols.

If the check box is cleared, the Web Threat Protection component 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 pre-configured 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 the Web Threat Protection component performs maximum scanning of web traffic that the computer receives over the HTTP and FTP protocols. Web Threat Protection performs detailed scanning of all web traffic objects by 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. The Web Threat Protection component 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. The Web Threat Protection component performs heuristic analysis at the **light scan** level.

Custom

Web traffic security level with your custom settings.

Settings

Clicking this button opens the **Web Threat Protection** 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 the Web Threat Protection component if scanning web traffic reveals that an object contains malicious code.

Block download

If this action is selected, on detecting an infected object in web traffic, the Web Threat Protection component blocks access to the object, displays a notification about the blocked access attempt, and makes a log entry with information about the infected object.

This action is selected by default.

Inform

If this option is selected and an infected object is detected in the web traffic, the Web Threat Protection component allows this object to be downloaded to the computer; Kaspersky Endpoint Security logs an event containing information about the infected object and adds information about the infected object to the list of active threats.

General tab

In this window, the administrator can select the scan methods used by the Web Threat Protection component, and configure the anti-phishing settings.

The following settings are available:

Check if links are listed in the database of malicious links

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 scan** and **Medium scan** 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 links are listed in the database of phishing links

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 web addresses 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 web addresses

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, the Web Threat Protection component does not scan the content of web pages or websites whose addresses are included in the list of trusted web addresses.

If the check box is cleared, the Web Threat Protection component scans the content of all opened web pages or websites.

This check box is selected by default.

Trusted web addresses

Contains the web addresses of web pages / websites whose content you trust. The Web Threat Protection component does not scan the content of web pages or 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 address of the web page or website is selected, the Web Threat Protection component does not scan the content of the web page or website.

If the check box next to the address of the web page or website is cleared, the Web Threat Protection component temporarily excludes the web address from the list of trusted web addresses and scans its content.

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, the Web Threat Protection component 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, the Web Threat Protection component interprets the address mask `Patch_123?.com` as any web address 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=`.

Mail Threat Protection

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 5).

This section contains information about the Mail Threat Protection component and instructions on how to configure the component settings.

In this section:

About Mail Threat Protection

The Mail Threat Protection component 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 email message, it becomes available and/or is processed.

When a threat is detected in an email message, the Mail Threat Protection component performs the following actions:

1. Assigns the *Infected* status to the email message.

   This status is assigned to the email message in the following cases:

   - A scan of the email message finds a section of code of a known virus that is included in the anti-virus databases of Kaspersky Endpoint Security.
   - The email message contains a section of code that is typical of viruses or other malware, or the modified code of a known virus.
2. Identifies the type of object detected in the email message (such as a *Trojan*).
3. Blocks the email message.
4. Displays a notification about the detected object (if configured to do so in the notification settings).
5. Performs the action defined in the Mail Threat Protection component settings.

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 Threat Protection extension is embedded in the Microsoft Office Outlook mail client during installation of Kaspersky Endpoint Security.

Mail Threat Protection subsection

Enable Mail Threat Protection

This check box enables / disables the Mail Threat Protection component.

When the check box is selected, the Mail Threat Protection component 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.

If the check box is cleared, the Mail Threat Protection component 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 pre-configured 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, the Mail Threat Protection component scans email messages most thoroughly. The Mail Threat Protection component scans incoming and outgoing email 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. The Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component 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

Clicking this button opens the **Mail Threat Protection** 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 Threat Protection performs if scanning reveals that an email message is infected.

> Before attempting to disinfect or delete an infected email message, the Mail Threat Protection component creates a backup copy of it so that the message can be restored or disinfected later.

Disinfect, delete if disinfection fails

If this option is selected, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component deletes the infected email messages.

This option is selected by default.

Disinfect, block if disinfection fails

If this option is selected, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component blocks the infected email messages.

Block

If this option is selected, the Mail Threat Protection component automatically blocks all infected email messages without attempting to disinfect them.

General tab

The **Protection scope** section allows you to select the type of email messages that are scanned by the Mail Threat Protection component.

Incoming and outgoing messages

If this setting is selected, the Mail Threat Protection component scans both incoming and outgoing email messages.

This is the default setting.

Incoming messages only

If this option is selected, the Mail Threat Protection component scans only incoming email messages.

The **Connectivity** section lets you configure the scanning of email traffic by the Mail Threat Protection component and the settings of Mail Threat Protection embedding into email clients.

POP3 / SMTP / NNTP / IMAP traffic

The check box enables / disables scanning by the Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component 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 Threat Protection component plug-in that is embedded in the 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 Threat Protection component settings from Microsoft Office Outlook and specify when the Mail Threat Protection component 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, the Mail Threat Protection component 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 the Mail Threat Protection component 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 the Mail Threat Protection component 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 the Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component analyzes each message as it arrives to the mailbox.

If the check box is cleared, the Mail Threat Protection component 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, the Mail Threat Protection component scans a message when the user opens it to read it.

If the check box is cleared, the Mail Threat Protection component 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, the Mail Threat Protection component analyzes each outgoing message as it is being sent.

If the check box is cleared, the Mail Threat Protection component 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 the Mail Threat Protection component will pick out email message attachments to undergo a virus scan.

> The Attachment filter functionality is not applied to outgoing email messages.

The following settings are available:

Disable filtering

If this setting is selected, the Mail Threat Protection component does not filter files that are attached to email messages.

This is the default setting.

Rename attachments of selected types

If this setting is selected, the Mail Threat Protection component replaces the last character in attached files of the specified types with the underscore (_) symbol.

Delete attachments of selected types

If this setting is selected, the Mail Threat Protection component 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 the Mail Threat Protection component either renames or deletes after filtering attachments in email messages.

The list of file masks is available if the **Rename attachments of selected types** option or the **Delete attachments of selected types** option is enabled.

If the check box next to the file mask is selected, the Mail Threat Protection component renames or deletes files of this type when filtering email attachments.

If the check box next to the file mask is cleared, the Mail Threat Protection component 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 the Mail Threat Protection component.

The following setting is available:

File mask

The file mask input field, in accordance with which the Mail Threat Protection component filters attachments in email messages.

Additional tab

In this window, the administrator can configure the heuristic analysis settings for the Mail Threat Protection component.

The following settings are available:

Heuristic Analysis

This check box enables or disables the use of heuristic analysis when email is scanned by the Mail Threat Protection component.

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 scan** and **Medium scan** 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.

BadUSB Attack Prevention subsection

Enable BadUSB Attack Prevention

This check box enables / disables the operation of the BadUSB Attack Prevention component.

This check box is selected by default.

Prohibit use of On-Screen Keyboard for authorization of USB devices

This check box enables or disables blocking of the use of On-Screen Keyboard for USB device authorization.

If the check box is selected, the application blocks use of On-Screen Keyboard for authorization of a USB device from which an authorization code cannot be entered.

If the check box is cleared, the application allows use of On-Screen Keyboard for authorization of a USB device from which an authorization code cannot be entered.

This check box is selected by default.

Application Control

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

In this section:

About Application Control

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

Startup of applications whose settings do not match any of the Application 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.

By default, Application Control operates in Black List mode. This component allows all users to start all applications. When a user attempts to start an application that is blocked by Application Control rules, Kaspersky Endpoint Security blocks this application from starting (if the **Block** action is selected) or saves information about the application startup in a report (if the **Notify** action is selected).

Application Control subsection

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

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

The following settings are available:

Application Control

This check box enables or disables the Application 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.

The check box is selected by default.

The **Application Control Settings** section lets you create application control rules and select the Application Control mode.

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 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 Control rule** window. You can create a new rule in this window.

Edit

Clicking this button opens the **Application 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.

Static analysis

This button opens the **Analysis of the access rights list** window. In this window, you can check whether the Application Control rules created in the current policy are working properly.

Application Control mode

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

You can choose one of the following items:

- **Black List**. If this item is selected, Application Control allows all users to start any applications, except in cases that satisfy the conditions of Application Control block rules.
- **White List**. If this item is selected, Application Control blocks all users from starting any applications, except in cases that satisfy the conditions of Application Control allow rules.

When **White list** mode is selected, two Application Control rules are automatically created:

- **Golden Image**.
- **Trusted Updaters**.

You cannot edit the settings of or delete automatically created rules. You can enable or disable these rules. By default, the **Golden Image** rule is enabled, and the **Trusted Updaters** rule is disabled.

The **Black List** item 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 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 Application Control mode, 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 an application that is blocked in the current Application Control mode, but logs information about its startup in the report.

The default option is **Block**.

Application Control rules

Table containing a list of Application Control rules.

The table contains the following columns:

- **Status**. This column displays the operating status of the rule. Left-clicking brings up a context menu in which you can select one of the following statuses:
  - **On**. This status means that the rule is used when the Application Control component is running.
  - **Off**. This status means that the rule is ignored when the Application Control component is running.
  - **Test**. This status means that Kaspersky Endpoint Security allows the startup of an application that is blocked in the current Application Control mode, but logs information about its startup in the report.

> You can use the **Test** status to specify the **Notify** action for some of the rules if the **Block** option is selected in the **Action** drop-down list.

- **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.

Control 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.

When enabling the function for controlling which DLL modules and drivers are loaded, make sure that the Application Control section has enabled the default Golden Image rule or another rule that contains the Trusted certificates KL category and ensures that trusted DLL modules and drivers are loaded before Kaspersky Endpoint Security is started. Enabling control of the loading of DLL modules and drivers when the Golden Image rule is disabled may cause instability in the operating system.

Kaspersky Endpoint Security monitors only DLL modules and drivers that are loaded after the Control DLL and drivers check box was selected. It is recommended to restart the computer after selecting the Monitor DLLs and drivers check box in order for Kaspersky Endpoint Security to monitor all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security starts.

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.

The **Advanced Settings** section lets you configure the templates for messages about blocking application startup and messages for the network administrator.

Templates

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

Blockage tab

The entry field contains the template of the message that is displayed when an Application 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 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 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 administrator.

Subject

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

The default subject is `[Application 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 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 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 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 information about which 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 Control rule window

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

An Application Control rule specifies the triggering conditions and the action performed by the Application Control component 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 Control rules:

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

An Application Control rule can be enabled (status: *On*) or disabled (status: *Off*). An Application Control rule is enabled by default after it is created.

- Delete rule

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

Rule name

Field for entering the name of the Application Control rule.

Description

This field lets you describe an application or group of applications for which an Application Control rule has been defined. You can leave this field empty.

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 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 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 into 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 into 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 Control rule.

The table contains the following columns:

- **Principal**. This column shows the users and/or user groups covered by the Application 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 **Principal** 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 **Principal** 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, subject, 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 Control performs the action prescribed in the rule. If application parameters match the values of criteria specified in the exclusion condition, Application Control does not control startup of the application.

To add a rule triggering condition, 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 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.

Application executable files

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 or excludes information about the executable file of an application from the condition that triggers the Application 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 or excludes information about the executable file of an application from the condition that triggers the Application Control rule.
- **Issuer**. This column shows the name of the application certificate issuer.
- **Principal**. 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 or excludes information about the executable file of an application from the condition that triggers the Application 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 or excludes information about the executable file of an application from the condition that triggers the Application 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 or excludes information about the executable file of an application from the condition that triggers the Application 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.

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.

KL category description

The lower part of the Condition(s) "KL category" window has a section containing brief information about the selected KL category, as well as a link to the web portal with a full description of this category.

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, subject, 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 Control performs the action prescribed in the rule. If application parameters match the values of criteria specified in the exclusion condition, Application 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.

Path to file or folder

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. In this window, you can select the folder containing the executable file of the application, based on which you want to create a condition that triggers an Application 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.

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 5).

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

In this section:

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.

Types of devices

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

- **Devices**. This column displays the names of the types of devices.
- **Access**. This column shows the status of access to the types of devices (*Allow*, *Block*, *Depends on bus, Restrict by rules*).

  A rule is assigned *Restrict by rules* access status if its status had been *Allow* 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.

Login.

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.

Import

Clicking this button imports a list of trusted devices from an XML file.

Export

Clicking this button exports the list of trusted devices or a subset of items in the list of trusted devices to an XML file.

Templates

This button opens the **Message 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 network administrator.

Anti-Bridging

Clicking this button opens the **Anti-Bridging** window. In this window, you can configure the Anti-Bridging settings.

Request access

This button opens the **Request access to device** window.

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 network 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 network 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 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 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.

Anti-Bridging window

Enable Anti-Bridging

This check box enables / disables Network Attack Blocker.

If the check box is selected, Kaspersky Endpoint Security blocks network bridges in accordance with the connection rules.

If the check box is cleared, Kaspersky Endpoint Security does not block network bridges.

This check box is cleared by default.

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.

The button is available if you have selected any item in the list of rules other than the top item.

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.

The button is available if you have selected any item in the list of rules other than the bottom item.

Rules for devices

Connection rules table. If the rule is used, Kaspersky Endpoint Security:

- Blocks the active connection when establishing a new connection, if the device type specified in the rule is used for both connections.
- Blocks connections established using the device types for which lower-priority rules are used.

The table contains the following columns:

- **Control**. This column displays one of the following rule statuses:
  - *En.* The rule is used.
  - *Dis.* The rule is not used.
- **Device type**. This column displays the type of device used to established the connection. This column displays one of the following predefined types of devices:
  - Network adapter.
  - Wi-Fi.
  - Modem.

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.

- **Disabled**.

  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 network 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

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 network 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.

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 5).

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

In this section:

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 specified categories of web resources (for example, block access to sites that belong to the "Internet communication" 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 the purposes of Kaspersky Lab applications 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.
- 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").
- Web resources with the following contents:
  - Articles and blogs covering sex education with both scientific and popular themes.
  - Medical encyclopedias, specifically their sections about sexual reproduction.
  - Resources of medical institutions, specifically their sections covering treatment of sexual organs.

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.
- 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.
- 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, obscenity

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.

Internet communication

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 and IM**.

  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" categories.

- **Web-based email**.

  This subcategory includes only 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.

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.

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.

Online stores, banks, 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:

- **Online stores**.

  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.

Anonymizers

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 network 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.
- 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.

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").

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.

Regional legal restrictions

This category includes the **Blocked as required by Russian Federation law** subcategory, which includes web resources that are blocked in accordance with the law of the Russian Federation.

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:

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.

The **Web Control Settings** section lets you generate rules for accessing web resources.

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.

The button is available if you have selected any item in the list of rules other than the top item.

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.

The button is available if you have selected any item in the list of rules other than the bottom item.

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of the **Rule name** or **Users** columns of the web resources access rule that you want to find in the **Access rules sorted by priority** table.

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

Access rules

Table with list of web resource access rules. The access rules are sorted in the table based on their priority. The higher the rule priority, the higher its position in the table.

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. The rule covers those users.
- **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 it is not recommended to visit the web resources listed in the rule while in the corporate network.

The **Advanced Settings** section lets you configure the templates for messages about blocking web resources and messages to the local corporate network administrator.

Templates

This button opens the **Message 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 network 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 network administrator.

Subject

The message subject is entered in this field.

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 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 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 website (%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 (see section "Web resource content categories" on page 109) 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 for 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.

Rule schedule window

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 for 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.

Managing Backup

This section contains instructions on how to configure and manage Backup.

In this section:

About Backup

Backup is a list of backup copies of files that have been deleted or modified during the disinfection process. A *backup copy* is a file copy created before the file was disinfected or deleted. Backup copies of files are stored in a special format and do not pose a threat.

Backup copies of files are stored in the folder ProgramData\Kaspersky Lab\KES\QB.

Users in the Administrators group are granted the permissions to access this folder. Limited access rights to this folder are granted to the user whose account was used to install Kaspersky Endpoint Security.

> Kaspersky Endpoint Security does not provide the capability to configure user access permissions to backup copies of files.

Sometimes it is not possible to maintain the integrity of files during disinfection. If you partially or completely lose access to important information in a disinfected file after disinfection, you can attempt to restore the file from its backup copy to its original folder.

If Kaspersky Endpoint Security is running under the management of Kaspersky Security Center, backup copies of files may be transmitted to the Kaspersky Security Center Administration Server. For more details about managing backup copies of files in Kaspersky Security Center, please refer to the Kaspersky Security Center Help system.

Configuring Backup settings

You can configure Backup settings as follows:

- Configure the maximum storage period for copies of files in Backup.

  The default maximum storage period for copies of files in Backup is 30 days. After expiration of the maximum storage term, Kaspersky Endpoint Security deletes the oldest files from Backup. You can cancel the time-based restriction or change the maximum file storage term.

- Configure the maximum size of Backup.

  By default, the maximum size of Backup is 100 MB. After the maximum size is reached, Kaspersky Endpoint Security automatically deletes the oldest files from Backup so that the maximum size is not exceeded. You can cancel the Backup size limit or change the maximum size.

In this section:

Configuring the maximum storage period for files in Backup

► *To configure the maximum storage period for files in Backup:*

1. Open the application settings window.
2. In the left part of the window, in the **General Settings** section, select **Reports and Storage**.
3. Do one of the following:
   - If you want to limit the storage period for copies of files in Backup, in the **Backup** 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 period for copies of files in Backup. The default maximum storage period for copies of files in Backup is 30 days.
   - If you want to cancel the storage period limit for copies of files in Backup, in the **Backup** section in the right part of the window, clear the **Store objects no longer than** check box.
4. To save changes, click the **Save** button.

Configuring the maximum size of Backup

► *To configure the maximum size of Backup:*

1. Open the application settings window.
2. In the left part of the window, in the **General Settings** section, select **Reports and Storage**.
3. Do one of the following:
   - If you want to limit the total size of Backup, select the **Maximum storage size** check box in the right part of the window in the **Backup** section and specify the maximum size of Backup in the field to the right of the **Maximum storage size** check box.

     By default, the maximum storage size for data comprising the backup copies of files is 100 MB.
   - If you want to remove the limit on the size of Backup, clear the **Maximum storage size** check box in the right part of the window in the **Backup settings** section.

   The size of Backup is unlimited by default.
4. To save changes, click the **Save** button.

Restoring and deleting files from Backup

If malicious code is detected in a file, Kaspersky Endpoint Security blocks the file, assigns the *Infected* status to it, 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 configured in 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.

  > For a backup copy of a file, the path to the original folder of the file is displayed. The path to the original folder of the file may contain personal data.

- 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 information about selected Backup files 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

> If several files with identical names and different content located in the same folder are moved to Backup, only the file that was last placed in Backup can be restored.

► *To restore files from Backup:*

1. Open the main application window.
2. Click the **Repositories** button in the lower part of the main application window.

   The **Backup** window opens.
3. If you want to restore all files from Backup, in the **Backup** window select **Restore all** from the context menu of any file.

   Kaspersky Endpoint Security restores all files from their backup copies to their original folders.
4. To restore one or more files from Backup :
   a. In the table in the **Backup** window, 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.

   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 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:*

1. Open the main application window.
2. Click the **Repositories** button in the lower part of the main application window.
3. The **Backup** window opens.
4. 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.
5. If you want to delete one or more files from Backup:
   a. In the table in the **Backup** window, 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.

   b. Delete files in one of the following ways:
      - Click the **Delete** button.

- Right-click to open the context menu and select **Delete**.

Kaspersky Endpoint Security deletes the selected backup copies of files from Backup.

Tasks

This section contains information about the specifics and settings of the scan tasks.

In this section:

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:*

1. Open the main application window.
2. Click the **Tasks** button in the lower part of the main application window.

   The **Tasks** window opens.
3. Click the section with the name of the scan task.

   The selected section is expanded.
4. Do one of the following:
   - Click the **Start** button if you want to run the scan task.

     The task progress status that is displayed under the name of this scan task changes to *Running*.
   - If you want to stop the scan task, select **Stop** in the context menu.

     The task progress status that is displayed under the name of this scan task changes to *Stopped*.

► *To start or stop a scan task when the simplified application interface is displayed (see section "Simplified application interface" on page 11):*

1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
2. In the **Tasks** drop-down list in the context menu, do one of the following:
   - select a non-running scan task to start it
   - select a running scan task to stop it
   - select a paused scan task to resume or restart it

Scan from context menu 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 into account.

High

If the probability of computer infection is very high, select this file security level.

If this option is selected, Kaspersky Endpoint Security uses the deep level of heuristic analysis.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists.

If this option is selected, Kaspersky Endpoint Security uses the medium level of heuristic analysis.

The **Recommended** file security level is selected by default.

Low

The settings of this file security level ensure maximum scanning speed.

If this option is selected, Kaspersky Endpoint Security uses the light level of heuristic analysis.

Custom

A file security level with your personal custom settings.

Settings

This button opens the Scan from context menu 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 Scan from context menu task detects infected files.

Disinfect, delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

This action is selected by default.

Disinfect, inform if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats.

Inform

If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.

Scope tab

The **File types** section lets you select the file types that Kaspersky Endpoint Security scans when performing scan tasks from context menu.

> 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 scan task from the context menu.

Scan only new and changed files

This check box enables / disables scanning only new files and files that have been modified since the last scan.

If scanning only new and modified files is enabled, the links for selecting in the **Scan of compound files** section (**all / new**) become unavailable.

Skip files that are scanned for 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**. The File Threat Protection component scans all archives.
- **New**. The File Threat Protection component scans only new archives that have been modified since the last scan.

  The setting is available if the **Scan only new and changed files** check box is cleared.

Scan distribution packages

The check box enables or disables scanning of distribution packages.

This check box is cleared by default.

The following scan options are available:

- **All**. The File Threat Protection component scans all distribution packages.
- **New**. The File Threat Protection component scans only new distribution packages that have been modified 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 or disables the function that the File Threat Protection component 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**. The File Threat Protection component scans all files in office formats.
- **New**. The File Threat Protection component scans only new Office format files that have been modified since the last 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.

Removable drives scan subsection

Action on connection of a removable drive

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 email message nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – saved Microsoft Office Outlook email message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file. 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

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 **Action on connection of a removable drive** drop-down list.

If this check box is selected, Kaspersky Endpoint Security performs the action that is selected in the **Action on connection of a removable drive** 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 **Action on connection of a removable drive** 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 **Action on connection of a removable drive** drop-down list.

This check box is cleared by default.

Show scan progress

This check box enables / disables display of the progress of removable drive scans in a separate window and in the **Tasks** window.

If the check box is selected, Kaspersky Endpoint Security displays the progress of removable drive scans in a separate window and in the **Tasks** window.

If the check box is cleared, Kaspersky Endpoint Security starts removable drive scans in the background.

This setting is available if the **Detailed Scan** or **Quick Scan** action is selected in the **Action on connection of a removable drive** drop-down list.

This check box is selected by default.

Background scan subsection

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.

Scan when the computer is idling

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.

General Settings

This section contains information about configuring the general settings of Kaspersky Endpoint Security.

In this section:

Application Settings subsection

The **Operating Mode** section lets you configure Kaspersky Endpoint Security to start when the computer is turned on, and enable or disable Advanced Disinfection technology.

Start Kaspersky Endpoint Security 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.

Enable Advanced Disinfection technology

> This check box is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. The check box 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 5).

This check box enables / disables the option whereby Kaspersky Endpoint Security uses advanced disinfection technology.

If the check box is selected, a pop-up notification is displayed on the screen when malicious activity is detected in the operating system. In its notification, Kaspersky Endpoint Security offers the user to perform Advanced Disinfection of the computer. After the user approves this procedure, Kaspersky Endpoint Security neutralizes the threat. 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, on detecting malicious activity in the operating system Kaspersky Endpoint Security carries out the disinfection procedure according to the current settings. No computer restart is performed after Kaspersky Endpoint Security neutralizes the threat.

This check box is selected by default.

The **Self-Defense** section lets you configure protection against external interference in the operation of the computer.

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 services

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 **Performance** section lets you configure optimum energy and computer resource consumption in the operation of Kaspersky Endpoint Security.

Postpone scheduled tasks while running on battery power

Computer scan tasks and database update tasks tend to consume considerable resources and take a long time to finish.

This check box enables / disables energy conservation mode when a portable computer is running on battery power, which postpones scan and update tasks.

If the check box is selected, energy conservation mode is enabled. Kaspersky Endpoint Security postpones scheduled tasks. The user can start scan and update tasks manually, if necessary.

If the check box is cleared, energy conservation mode is disabled. Scan and update tasks are started according to their respective schedules.

This check box is selected by default.

Concede resources to other applications

When Kaspersky Endpoint Security runs scheduled tasks, this may result in increased workload on the CPU and disk subsystems, which slows down the performance of other applications.

When the check box is selected, Kaspersky Endpoint Security suspends scheduled tasks when it detects an increased load and frees up operating system resources for user applications. This helps to relieve the load on the CPU and disk subsystems.

When the check box is cleared, scheduled tasks are performed without regard for the operation of other applications.

This check box is selected by default.

The **Proxy Server** section allows you to configure the connection to a proxy server used to connect to the Internet.

Settings

Clicking the button opens the **Proxy server settings** window. This window lets you configure the proxy server used for Internet access.

The **Debug Information** section allows you to configure settings for working with dump and trace files.

Settings

Clicking this button opens the **Debug information** window. In this window, you can configure the settings for working with dump files and trace files.

Proxy Server Settings window

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 address

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.

Debug information window

Enable dump writing

Writing of dump files that can be used to examine Kaspersky Endpoint Security crashes.

If the check box is selected, Kaspersky Endpoint Security writes dumps when it crashes.

If the check box is cleared, Kaspersky Endpoint Security does not write dumps. The application also deletes existing dump files from the computer hard drive.

This check box is selected by default.

Enable dump and trace files protection

This check box enables / disables protection of dump files and trace files.

If the check box is selected, access to dump files is granted to the system and local administrators as well as to the user who enabled dump or trace file writing. Only system and local administrators can access trace files.

If the check box is cleared, any user can access dump files and trace files.

This check box is selected by default.

Exclusions subsection

The **Objects for detection** section lets you select the types of objects that Kaspersky Endpoint Security should monitor while it is running.

Settings

This button opens the **Objects for detection** window. In this window, you can modify the list of objects 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 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 exclusions 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 a list of exclusions 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 the File Threat Protection, Web Threat Protection, and Mail Threat Protection components 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 only selected ports

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 and 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.

Trojan

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 **Packers** 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
- Selected files
- Folders
- Files and folders that are selected by a mask

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

> Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
> The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.

- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

- 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.
- **Object hash**. This column shows the SHA256 hash 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 malware detects an object with the specified hash.
- **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 **Scan exclusion** window. You can create a new exclusion in this window.

Edit

Clicking this button opens the **Scan exclusion** window. You can edit the settings of the selected exclusion in this window.

This button is available when an item is selected in the **Scan exclusions** 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 exclusions 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.

Object hash

This check box enables / disables the option that excludes a file with the specified hash from the virus scan.

Comment

A field for entering additional information about the exclusion.

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 during scans. You can also define a file or folder name mask.

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

> Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
> The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

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.

Object hash: enter the object hash

Clicking this link opens the **Object hash** window. In this window, you can define the SHA256 hash of an object to exclude from scanning.

Protection components: any / specified: select components

The **any** option signifies that this exclusion is used by all components of Kaspersky Endpoint Security.

The **specified** option 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** option is available if the **specified** option is available.

The **any** option 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.

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.

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:

Name of file or folder

Field for entering the file or folder name, or the mask of the file or folder name.

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

> Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
> The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

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

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\test** – Only the file C:\dir\test.

Browse

This button opens the **Select folder** window. You can select a file or folder in this window.

Include subfolders

This check box enables / disables an option whereby a folder is added to the exclusion 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.

Scan exclusions tab

Scan exclusions

This table contains information about scan exclusions.

You can exclude the following objects from scanning:

- Files of certain formats
- Selected files
- Folders
- Files and folders that are selected by a mask

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

> Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
> The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

- 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.
- **Object hash**. This column shows the SHA256 hash 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 malware detects an object with the specified hash.
- **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 **Scan exclusion** window. You can create a new exclusion in this window.

Edit

Clicking this button opens the **Scan exclusion** window. You can edit the settings of the selected exclusion in this window.

This button is available when an item is selected in the **Scan exclusions** 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.

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 Application Control component regulates the startup of each of the applications regardless of whether or not the application is included in the table of trusted applications.

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 or disables the scan exclusion for all files opened by the specific application.

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 or disables monitoring of the file- and network activity of an application in the operating system by the Host Intrusion Prevention, Behavior Detection, Exploit Prevention, Remediation Engine 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 or disables the scan exclusion for network traffic generated by the specific application.

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 scan exclusion settings for network traffic.

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 Host Intrusion Prevention 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 Host Intrusion Prevention 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 **Select file or folder** window. 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 for Windows Administration Plug-in to generate a list of applications whose network activity should be monitored by Firewall via the 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.

Reports and Storage subsection

The **Reports** section lets you configure the application report storage settings.

Store reports no longer than

This check box enables / disables the option that defines the maximum report storage term. The maximum report storage term is measured in days.

When the check box is selected, the maximum storage term is limited by the amount of time that is specified in the field on the right. The default maximum storage term for reports is 30 days. After that period of time, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file.

This check box is selected by default.

Maximum file size

The check box enables / disables the option that defines the maximum report file size. The maximum report file size is specified in megabytes.

When the check box is selected, the maximum report file size is limited by the value that is specified in the field on the right. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file when the maximum report file size is reached.

This check box is selected by default.

Delete reports

Clicking this button opens the **Delete reports** window. This window lets you select the reports that you want to clear.

The **Backup** section lets you configure Backup settings.

Store objects no longer than

This check box enables / disables the option that defines the maximum storage period for copies of files in Backup. The maximum file storage term is measured in days.

When the check box is selected, the maximum storage term for files is limited by the amount of time that is specified in the field on the right. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Endpoint Security deletes the oldest files from Backup.

This check box is selected by default.

Maximum storage size

The check box enables / disables the option that defines the maximum data storage size. The data storage comprises storage for backup copies of files. The maximum size of the data storage is specified in megabytes.

When the check box is selected, the maximum storage size is limited by the value that is specified in the field on the right. By default, the maximum size is 100 MB. To not exceed the maximum data storage size, Kaspersky Endpoint Security automatically deletes the oldest files when the data storage reaches its maximum size.

This check box is cleared by default.

Delete Reports window

All reports

The check box enables / disables deletion of information from all Kaspersky Endpoint Security reports.

This check box is cleared by default.

Protection components report

This check box enables / disables deletion of information about the operation of the following Kaspersky Endpoint Security components:

- Behavior Detection.
- Exploit Prevention.
- Host Intrusion Prevention.
- File Threat Protection.
- Web Threat Protection.
- Mail Threat Protection.
- Network Threat Protection.
- BadUSB Attack Prevention.

The amount of space that the report uses on the hard drive is shown for the report.

This check box is cleared by default.

Control components report

This check box enables / disables deletion of information about the operation of the following Kaspersky Endpoint Security components:

- Application Control.
- Device Control.
- Web Control.

The amount of space that the report uses on the hard drive is shown for the report.

This check box is selected by default.

Data encryption report

The check box enables / disables the deletion of information about completed data encryption tasks.

The amount of space that the report uses on the hard drive is shown for the report.

This check box is selected by default.

Scan tasks report

The check box enables / disables the deletion of information about completed scan tasks:

- Full Scan.
- Critical Areas Scan.
- Custom Scan.
- Integrity Check.

The amount of space that the report uses on the hard drive is shown for the report.

This check box is selected by default.

Update task report

This check box enables / disables deletion of information about the completed update tasks of Kaspersky Endpoint Security.

The amount of space that the report uses on the hard drive is shown for the report.

This check box is selected by default.

Firewall report

This check box enables / disables the deletion of information about processing of network rules by Firewall.

The amount of space that the report uses on the hard drive is shown for the report.

This check box is selected by default.

Manage Settings subsection

The **Saving current settings** section lets you save a configuration file with Kaspersky Endpoint Security settings.

Save

Clicking this button opens the **Please select a configuration file** window in Microsoft Windows. This window lets you save a configuration file with Kaspersky Endpoint Security settings.

The **Loading saved settings** section lets you load a configuration file with Kaspersky Endpoint Security settings.

Load

Clicking this button opens the **Please select a configuration file** window in Microsoft Windows. This window lets you load a configuration file with Kaspersky Endpoint Security settings.

The **Restoring default settings** section lets you return to the Kaspersky Endpoint Security default settings.

Restore

Clicking this button opens the Initial Configuration Wizard. The Initial Configuration Wizard can be used to revert Kaspersky Endpoint Security to its default settings.

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 network 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 network 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 policy or disable encryption in the Kaspersky Security Center policy settings on the computer where the procedure will be performed. This prevents the drive from being encrypted again.

In this section:

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 to administrator the request access file with the kesdc extension for the encrypted device. To do so, perform one of the following:

   - To email the network 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 network 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 network 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 network 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 **Support** 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 stand-alone Restore Utility** button in the window of Restore Utility.

   The **Creating stand-alone 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 stand-alone 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 **Support** button in the main window of Kaspersky Endpoint Security to open the **Support** window and click the **Restore encrypted device** button.

   - Run the executable fdert.exe file of Restore Utility. This file is created using Kaspersky Endpoint Security (see section "Creating the executable file of Restore Utility" on page 160).

2. In the Restore Utility window, from the **Select device** drop-down 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:

   a. Select the **Use Authentication Agent account settings** option.

   b. 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 network administrator to restore data on an encrypted device.

7. If you want to use an access key to restore data:

a. Select the **Specify device access key manually** option.

b. Click the **Receive access key** button.

c. The **Receive device access key** window opens.

d. Click the **Save** button and select the folder in which to save the request access file with the fdertc extension.

e. Send the request access file to the network 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.

f. Obtain and save the access key file that was created and provided to you by the network administrator.

g. 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 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 network 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 receiving access to encrypted devices or restoring data on encrypted devices (see section "Working with encrypted devices when there is no access to them" on page 158).

In this section:

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 164).

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 network 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

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 network 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 network administrator.

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 network 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 receiving access to encrypted devices or restoring data on encrypted devices (see section "Working with encrypted devices when there is no access to them" on page 158).

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

Kaspersky Security Center lets you remotely install and uninstall, start and stop Kaspersky Endpoint Security, configure application settings, change the set of available application components, add keys, and start and stop update and scan tasks.

In the section about Application Control, you can find information about managing Application Control rules using Kaspersky Security Center.

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 help.

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 Help Guide.

In this section:

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.

The ability to change application settings on the client computer is determined by the status of the "lock" on these settings in the policy properties:

- A closed “lock” (🔒) means the following:
  - Kaspersky Security Center blocks changes to settings that this lock relates to from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
  - Kaspersky Security Center blocks changes to settings that this lock relates to in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

- An open “lock” (🔓) means the following:
  - Kaspersky Security Center allows changes to settings that this lock relates to from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
  - Kaspersky Security Center allows changes to settings that this lock relates to in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

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:

- Essential Threat Protection. The functional scope includes the File Threat Protection, Mail Threat Protection, Web Threat Protection, Network Threat Protection, Firewall, and Scan Task components.
- Application Control. The functional scope includes the Application Control component.
- Device Control. The functional scope includes the Device Control component.
- Encryption. The functional scope includes the Full Disk Encryption and File Level Encryption components.
- Trusted zone. The functional scope includes the Trusted Zone.
- Web Control. The functional scope includes the Web Control component.
- Advanced Threat Protection. The functional scope includes KSN settings and the Behavior Detection, Exploit Prevention, Host Intrusion Prevention, and Remediation Engine components.
- Basic functionality. This functional scope includes general application settings that are not specified for other functional scopes, including: licensing, inventory tasks, application database and module update tasks, Self-Defense, advanced application settings, reports and storages, password protection 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 Help 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 configuration section

The **Event configuration** section allows you to configure event logging and event notifications. Events are distributed by importance level on the following tabs:

- **Critical event**. The **Critical event** tab is not displayed in the Network Agent policy properties.
- **Functional failure**.
- **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.

To select multiple event types, use the SHIFT or CTRL key; to select all types, use the **Select all** button.

Kaspersky Security Network is not available.

Kaspersky Security Network

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.

The check box remains selected or cleared depending on what was chosen during the initial configuration of Kaspersky Endpoint Security

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

KSN Statement

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 Settings** section lets you configure the Administration Console to display the statuses of client computers with Kaspersky Endpoint Security installed.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is open by default.

Enable extended KSN mode

The check box enables / disables extended Kaspersky Security Network (KSN) mode in the operation of Kaspersky Endpoint Security. The use of KSN is voluntary.

If the check box is selected, Kaspersky Endpoint Security sends its operation statistics to the KSN server and can send to Kaspersky Lab for additional analysis any files (or parts of files) that can be used by intruders to harm the computer or data.

If the check box is cleared, Kaspersky Endpoint Security uses basic KSN functions.

The check box remains selected or cleared depending on what was chosen during the initial configuration of Kaspersky Endpoint Security

Enable cloud mode for protection components

This check box enables or disables cloud mode for protection components.

If the check box is selected, Kaspersky Endpoint Security uses the light version of anti-virus databases, which reduces the load on operating system resources.

Kaspersky Endpoint Security downloads the light version of anti-virus databases during the next update after the check box was selected.

If the check box is cleared, Kaspersky Endpoint Security uses the full version of anti-virus databases.

Kaspersky Endpoint Security downloads the full version of anti-virus databases during the next update after the check box was cleared.

This check box is selected by default.

When cloud mode is enabled

The items in this drop-down list determine which computer status is displayed in the Administration Console when cloud mode is enabled.

You can select the following list items:

- OK
- **Warning**.
- **Critical**.

This drop-down list is available if the **Enable cloud mode for protection components** check box is selected.

The **Critical** item is selected by default.

When cloud mode is disabled

The items in this drop-down list determine which computer status is displayed in the Administration Console when cloud mode is enabled.

You can select the following list items:

- OK
- **Warning**.
- **Critical**.

This drop-down list is available if the **Enable cloud mode for protection components** check box is cleared.

The **Warning** item is selected by default.

The **KSN Proxy Settings** section lets you configure the KSN Proxy settings.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is open 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.

Behavior Detection section

Behavior Detection

This check box enables / disables the Behavior Detection component.

If the check box is selected, Kaspersky Endpoint Security monitors the activity of applications in the system and provides information about the activity of these applications to other components for more effective protection.

If the check box is cleared, Kaspersky Endpoint Security does not monitor the activity of applications in the system.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **On detecting malware activity** section lets you configure the action to be taken by the Behavior Detection component when it detects malware activity.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

On detecting malware activity

The items in this drop-down list determine the possible actions taken by Kaspersky Endpoint Security when it detects malicious activity:

- **Delete file**. If this item is selected, on detecting malicious activity Kaspersky Endpoint Security deletes the executable file of the malicious application and creates a backup copy of the file in Backup.
- **Terminate the program**. If this item is selected, on detecting malicious activity Kaspersky Endpoint Security terminates this application.
- **Inform**. If this item is selected and malware activity of an application is detected, Kaspersky Endpoint Security adds information about the malware activity of the application to the list of active threats.

The **Delete file** option is selected by default.

The **Protection of shared folders against external encryption** section lets you configure the settings for the function that protects shared folders against external encryption.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is open by default.

Enable protection of shared folders against external encryption

The check box enables or disables protection of shared folders against external encryption.

If the check box is selected, Kaspersky Endpoint Security monitors the following operations performed from a remote computer:

- Deletion of a file
- Modification of file contents
- Modification of file size
- Movement of a file.

If the check box is cleared, Kaspersky Endpoint Security does not monitor the following operations performed from a remote computer.

This check box is cleared by default.

On detection of external encryption of shared folders

The items in this drop-down list determine the possible actions taken by Kaspersky Endpoint Security when it detects attempts to encrypt shared folders from a remote computer:

- **Block connection**. If this item is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security blocks network activity originating from the computer attempting to modify files and creates backup copies of modified files.

If the Remediation Engine component is enabled and the **Block connection** option is selected, Kaspersky Endpoint Security restores modified files from backup copies.

- **Inform**. If this item is selected, on detecting an attempt to modify files in shared folders, Kaspersky Endpoint Security adds information about this attempt to modify files in shared folders to the list of active threats.

Kaspersky Endpoint Security prevents external encryption of only those files that are located on media that have the NTFS file system and are not encrypted by the EFS system.

The **Block connection** option is selected by default.

Block connection for

The time for which Kaspersky Endpoint Security blocks the network activity of the remote computer performing encryption of shared folders.

The default value is 60 minutes.

Exclusions

The Audit Logon service must be enabled to enable the list of computers excluded from protection of shared folders against external encryption. By default, the Audit Logon service is disabled (for detailed information about enabling the Audit Logon service, please visit the Microsoft website).

Clicking the button opens the **Exclusions** window. This window lets you create a list of IP addresses of remote computers from which attempts to modify files in shared folders will not be monitored.

Exclusions window

The Audit Logon service must be enabled to enable the list of computers excluded from protection of shared folders against external encryption. By default, the Audit Logon service is disabled (for detailed information about enabling the Audit Logon service, please visit the Microsoft website).

Add

Clicking this button opens the **Computers** window. This window lets you add the IP address or name of a computer to the list of exclusions.

Edit

Clicking this button opens the **Computers** window. In this window, you can edit the IP address or name of a computer in the list of exclusions.

This button is available if an item is selected in the list of exclusions.

Delete

Clicking this button causes Kaspersky Endpoint Security to remove the selected item from the list of exclusions.

The button is available if you have selected any item in the list of exclusions.

Computers

List of computers from which attempts to encrypt shared folders will not be monitored.

Computers window

Field for entering the name or IP address of the computer.

Exploit Prevention section

Exploit Prevention

This check box enables / disables the Exploit Prevention component.

If the check box is selected, Kaspersky Endpoint Security keeps track of executable files launched by vulnerable applications.

If the check box is deselected, Kaspersky Endpoint Security does not keep track of executable files launched by vulnerable applications.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **On detecting exploit** section lets you configure the action to be taken by the Exploit Prevention component when it detects the startup of an executable file of a vulnerable application.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

On detecting exploit

The items in this drop-down list determine the possible actions taken by Kaspersky Endpoint Security on detection of an exploit:

- **Block operation**. If this item is selected, on detection of an exploit Kaspersky Endpoint Security blocks all operations attempted by the exploit.
- **Inform**. If this item is selected and an exploit is detected, Kaspersky Endpoint Security adds information about this exploit to the list of active threats.

The **Block operation** option is selected by default.

The **System processes memory protection** section lets you enable or disable monitoring of attempts by external processes to access system processes.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Enable system process memory protection

This check box enables / disables protection of system process memory.

If this check box is selected, Kaspersky Endpoint Security blocks external processes that attempt to access system process memory.

If this check box is cleared, Kaspersky Endpoint Security does not block external processes that attempt to access system process memory.

This check box is selected by default.

Host Intrusion Prevention

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 5).

This section contains information about Host Intrusion Prevention and instructions on how to configure the component settings.

In this section:

About Host Intrusion Prevention

The Host Intrusion Prevention component prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources and personal 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 privilege 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, the Host Intrusion Prevention component checks the security of the application and places it into one of the trust groups. A trust group defines the rules that Kaspersky Endpoint Security applies when controlling application activity.

You are advised to participate in Kaspersky Security Network to improve the performance of the Host Intrusion Prevention component (see section "Participation in Kaspersky Security Network" on page 12). Data that is obtained through Kaspersky Security Network allows you to sort applications into groups with more accuracy and to apply optimum application privilege control rules.

The next time the application starts, Host Intrusion Prevention verifies the integrity of the application. If the application is unchanged, the component applies the current application privilege control rules to it. If the application has been modified, Host Intrusion Prevention analyzes the application as if it were being started for the first time.

Host Intrusion Prevention section

Host Intrusion Prevention

This check box enables or disables the operation of the Host Intrusion Prevention component.

If the check box is selected, the Host Intrusion Prevention component starts at Kaspersky Endpoint Security startup and registers the activity of applications in the system.

If the check box is cleared, the Host Intrusion Prevention component is disabled.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **Application rules** section lets you create application privilege control rules.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the

Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.

- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings (Applications)

Clicking this button opens the **Application privilege control** tab in the **Host Intrusion Prevention** window. This tab shows the list of applications, access to which is monitored by the Host Intrusion Prevention component. Applications are assigned to trust groups.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 user has placed applications in the Untrusted group.

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

Settings (Resources)

This button opens the **Protected resources** tab in the **Applications** window. On this tab, you can view the list of personal data and operating system settings and resources to which the Host Intrusion Prevention component controls access. You can also enable the protection of any resources in the list or add other resources to the list.

The **Application processing rules** section lets you configure rules for assigning applications to trust groups.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Update control rules for previously unknown applications from KSN databases

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

If the check box is selected, the Host Intrusion Prevention component updates the application privilege 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, the Host Intrusion Prevention component places digitally signed applications in the Trusted group.

If this check box is cleared, the Host Intrusion Prevention component 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.

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

This check box enables / disables the option to automatically delete application privilege 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 the Host Intrusion Prevention component deletes the application privilege control rules of applications that have not been started for more than 60 days.

If trust group cannot be defined, automatically move applications to

Items in this drop-down list determine to which trust group Kaspersky Endpoint Security will assign an unknown application.

You can choose one of the following items:

- **Low Restricted**.
- **High Restricted**.
- **Untrusted**.

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 privilege control 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

Table of application privilege control rules for applications that are categorized into trust groups. Kaspersky Endpoint Security applies the application privilege control rules to regulate applications' access to operating system processes and resources.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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 privilege 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 applications 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 Host Intrusion Prevention and File Threat Protection 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 the Host Intrusion

Prevention component 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 **Configure application privilege 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.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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.

Geographic spread

Popularity of the application among Kaspersky Security Network participants by country.

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 ⊞ and ⊟ 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 or disables the scan exclusion for all files opened by the specific application.

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 or disables monitoring of the file- and network activity of an application in the operating system by the Host Intrusion Prevention, Behavior Detection, Exploit Prevention, Remediation Engine 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 or disables the scan exclusion for network traffic generated by the specific application.

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 scan exclusion settings for network traffic.

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 the Host Intrusion Prevention component 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. The Host Intrusion Prevention component 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, the Host Intrusion Prevention component protects the resource.

If the check box next to a resource is cleared, the Host Intrusion Prevention component 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, in addition to 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 the resources that the user has excluded from the protection scope of the Host Intrusion Prevention component. 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, the Host Intrusion Prevention component does not control access to this resource.

If the check box next to a resource is cleared, the Host Intrusion Prevention component 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 must be protected by Application 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\* – 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 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` key 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 must be protected by the Host Intrusion Prevention component.

The Host Intrusion Prevention component 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.

Kaspersky Endpoint Security categorizes all applications that are started on the computer into trust groups. Applications are categorized 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 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 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 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.

Remediation Engine section

Remediation Engine

This check box enables / disables the Remediation Engine component.

If the check box is selected, when Kaspersky Endpoint Security detects malicious applications it rolls back the actions of these applications in the operating system.

If the check box is cleared, Kaspersky Endpoint Security does not roll back the actions of these applications in the operating system.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.
- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is

the same as the status that is defined in the top level policy properties.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

File Threat Protection section

File Threat Protection

This check box enables or disables the File Threat Protection component.

If the check box is selected, the File Threat Protection component 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, the File Threat Protection component is configured with the settings that are recommended by Kaspersky Lab experts.

If the check box is cleared, File Threat Protection is disabled.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed 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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

High

When this file security level is selected, the File Threat Protection component takes the strictest control of all files that are opened, saved, and started. The File Threat Protection component scans all file types on all hard drives, removable drives, and network drives 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. The File Threat Protection component scans only the specified file formats on all hard drives, removable drives, and network drives of the computer, and embedded OLE objects. The File Threat Protection component 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. The File Threat Protection component scans only files with specified extensions on all hard drives, removable drives, and network drives of the computer. The File Threat Protection component does not scan compound files.

Custom

A file security level with your personal custom settings.

Settings

Clicking this button opens the **File Threat Protection** window. In this window, you can configure file security level settings.

By default

This button sets the file security level to **Recommended**.

In the **Action on threat detection** section, you can select the action that the File Threat Protection component performs if infected files are detected when scanning.

> Before attempting to disinfect or delete an infected file, the File Threat Protection component creates a backup copy in case it becomes necessary to restore the file or it becomes possible to disinfect the file at a later time.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.

- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Disinfect, delete if disinfection fails

If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component deletes these files.

This option is selected by default.

Disinfect, block if disinfection fails

If this option is selected, the File Threat Protection component automatically attempts to disinfect all infected files that are detected. If disinfection fails, the File Threat Protection component blocks these files.

Block

If this option is selected, the File Threat Protection component automatically blocks all infected files without attempting to disinfect them.

About File Threat Protection

The File Threat Protection component lets you prevent infection of the file system of the computer. By default, the File Threat Protection component starts together with Kaspersky Endpoint Security, continuously resides in the computer's RAM, and scans files that are opened or run on the computer and on its attached drives to find viruses and other potential threats. The scan is performed according to the application settings.

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. 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 Threat Protection component settings.

General tab

The **File types** section allows you to select the types of files that the File Threat Protection component scans.

> The File Threat Protection component assumes that files without an extension are executable files. The File Threat Protection component always scans executable files, regardless of the file types that are selected for scanning.

All files

If this setting is selected, the File Threat Protection component scans all files without exception (all formats and extensions).

Files scanned by format

If this setting is selected, the File Threat Protection component scans infectable files only.

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, the File Threat Protection component scans infectable files only. 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 the File Threat Protection component.

The **Protection scope** section allows you to create a list of objects that are scanned by the File Threat Protection component.

Protection scope

Contains objects that are scanned by the File Threat Protection component. A scan object may be a hard drive or network drive, folder, file, or file name mask.

By default, the File Threat Protection component scans files that are started on any hard drives, removable drives, or network 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, the File Threat Protection component scans it.

If the check box next to the name of a scan object is cleared, the File Threat Protection component 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 the File Threat Protection component.

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

Clicking 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 Threat Protection** 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, the File Threat Protection component 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.

The File Threat Protection component 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 the File Threat Protection component uses when scanning the computer.

Machine learning and signature analysis

The machine learning and signature analysis method uses the Kaspersky Endpoint Security databases that contain descriptions of known threats and ways to neutralize them. Protection that uses this method provides the minimum acceptable security level.

Based on the recommendations of Kaspersky Lab experts, machine learning and signature analysis 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 heuristic analysis level. The heuristic analysis level ensures a 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 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 heuristic analysis level, the probability of detecting threats is lower than at the **medium scan** and **deep scan** heuristic analysis levels. Scanning is faster and less resource-intensive.

  The **Light scan** heuristic analysis level is selected 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** levels of heuristic analysis. At this heuristic analysis level, the probability of detecting threats is higher than at the **Light scan** and **Medium scan** levels of heuristic analysis. 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. The File Threat Protection component scans both simple 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 the File Threat Protection component scans for viruses and other 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**. The File Threat Protection component scans all archives.
- **New**. The File Threat Protection component scans only new archives that have been modified since the last scan.

  The setting is available if the **Scan only new and changed files** check box is cleared.

Scan installation packages

The check box enables or disables scanning of distribution packages.

This check box is cleared by default.

The following scan options are available:

- **All**. The File Threat Protection component scans all distribution packages.
- **New**. The File Threat Protection component scans only new distribution packages that have been modified 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 or disables the function that the File Threat Protection component 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**. The File Threat Protection component scans all files in office formats.
- **New**. The File Threat Protection component scans only new Office format files that have been modified since the last 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.

Unpack 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 the File Threat Protection component.

Smart mode

In this scan mode, the File Threat Protection component 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, the File Threat Protection component 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, the File Threat Protection component 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, the File Threat Protection component 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 run the files.

The **Scan technologies** section contains scan technologies that the File Threat Protection component 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 the File Threat Protection component.

By schedule

The check box enables or disables the function that lets you pause the File Threat Protection component for a specified amount of 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 the File Threat Protection component is paused.

The button is available if the **By schedule** check box is selected.

At application startup

This check box enables or disables the function that pauses the File Threat Protection component while the user works with applications that require significant resources of 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 require the File Threat Protection component to be paused 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 the File Threat Protection component.

The following settings are available:

Pause task at

Field for entering the time at which the File Threat Protection component is paused. The time is specified in HH:MM format.

Resume task at

Field for entering the time at which the File Threat Protection component is resumed. 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 the File Threat Protection component to terminate its operation.

The following settings are available:

Applications

This list includes applications during whose operation Kaspersky Endpoint Security pauses the operation of the File Threat Protection component. 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 the File Threat Protection component 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.

Web Threat Protection section

Web Threat Protection

This check box enables or disables the operation of the Web Threat Protection component.

If the check box is selected, the Web Threat Protection component protects information that arrives on the computer over the HTTP and FTP protocols.

If the check box is cleared, the Web Threat Protection component is disabled.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* /

Disabled) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **Security level** section allows you to select one of three security levels for web traffic that are pre-configured 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 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

High

The security level under which the Web Threat Protection component performs maximum scanning of web traffic that the computer receives over the HTTP and FTP protocols. Web Threat Protection performs detailed scanning of all web traffic objects by 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. The Web Threat Protection component 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. The Web Threat Protection component performs heuristic analysis at the **light scan** level.

Custom

Web traffic security level with your custom settings.

Settings

Clicking this button opens the **Web Threat Protection** 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 the Web Threat Protection component if scanning web traffic reveals that an object contains malicious code.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Block download

If this action is selected, on detecting an infected object in web traffic, the Web Threat Protection component blocks access to the object, displays a notification about the blocked access attempt, and makes a log entry with information about the infected object.

This action is selected by default.

Inform

If this option is selected and an infected object is detected in the web traffic, the Web Threat Protection component allows this object to be downloaded to the computer; Kaspersky Endpoint Security logs an event containing information about the infected object and adds information about the infected object to the list of active threats.

General tab

In this window, the administrator can select the scan methods used by the Web Threat Protection component, and configure the anti-phishing settings.

The following settings are available:

Check if links are listed in the database of malicious links

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 scan** and **Medium scan** 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 links are listed in the database of phishing links

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 web addresses 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 web addresses

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, the Web Threat Protection component does not scan the content of web pages or websites whose addresses are included in the list of trusted web addresses.

If the check box is cleared, the Web Threat Protection component scans the content of all opened web pages or websites.

This check box is selected by default.

Trusted web addresses

Contains the web addresses of web pages / websites whose content you trust. The Web Threat Protection component does not scan the content of web pages or 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 address of the web page or website is selected, the Web Threat Protection component does not scan the content of the web page or website.

If the check box next to the address of the web page or website is cleared, the Web Threat Protection component temporarily excludes the web address from the list of trusted web addresses and scans its content.

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, the Web Threat Protection component 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, the Web Threat Protection component interprets the address mask `Patch_123?.com` as any web address 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=`.

Mail Threat Protection section

Mail Threat Protection

This check box enables / disables the Mail Threat Protection component.

When the check box is selected, the Mail Threat Protection component 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.

If the check box is cleared, the Mail Threat Protection component is disabled.

This check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **Security level** section allows you to select one of three email security levels that are pre-configured 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 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the

Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.

- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

High

When this email security level is selected, the Mail Threat Protection component scans email messages most thoroughly. The Mail Threat Protection component scans incoming and outgoing email 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. The Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component 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

Clicking this button opens the **Mail Threat Protection** 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 Threat Protection performs if scanning reveals that an email message is infected.

> Before attempting to disinfect or delete an infected email message, the Mail Threat Protection component creates a backup copy of it so that it can be restored or disinfected later.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Disinfect, delete if disinfection fails

If this option is selected, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component deletes the infected email messages.

This option is selected by default.

Disinfect, block if disinfection fails

If this option is selected, the Mail Threat Protection component automatically attempts to disinfect all infected email messages that are detected. If disinfection fails, the Mail Threat Protection component blocks the infected email messages.

Block

If this option is selected, the Mail Threat Protection component automatically blocks all infected email messages without attempting to disinfect them.

General tab

The **Protection scope** section allows you to select the type of email messages that are scanned by the Mail Threat Protection component.

Incoming and outgoing messages

If this setting is selected, the Mail Threat Protection component scans both incoming and outgoing email messages.

This is the default setting.

Incoming messages only

If this option is selected, the Mail Threat Protection component scans only incoming email messages.

The **Connectivity** section lets you configure the scanning of email traffic by the Mail Threat Protection component and the settings of Mail Threat Protection embedding into email clients.

POP3 / SMTP / NNTP / IMAP traffic

The check box enables / disables scanning by the Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component 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 Threat Protection component plug-in that is embedded in the 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 Threat Protection component settings from Microsoft Office Outlook and specify when the Mail Threat Protection component 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, the Mail Threat Protection component 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 the Mail Threat Protection component 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 the Mail Threat Protection component 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 the Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component 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, the Mail Threat Protection component analyzes each message as it arrives to the mailbox.

If the check box is cleared, the Mail Threat Protection component 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, the Mail Threat Protection component scans a message when the user opens it to read it.

If the check box is cleared, the Mail Threat Protection component 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, the Mail Threat Protection component analyzes each outgoing message as it is being sent.

If the check box is cleared, the Mail Threat Protection component 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 the Mail Threat Protection component will pick out email message attachments to undergo a virus scan.

> The Attachment filter functionality is not applied to outgoing email messages.

The following settings are available:

Disable filtering

If this setting is selected, the Mail Threat Protection component does not filter files that are attached to email messages.

This is the default setting.

Rename attachments of selected types

If this setting is selected, the Mail Threat Protection component replaces the last character in attached files of the specified types with the underscore (_) symbol.

Delete attachments of selected types

If this setting is selected, the Mail Threat Protection component 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 the Mail Threat Protection component either renames or deletes after filtering attachments in email messages.

The list of file masks is available if the **Rename attachments of selected types** option or the **Delete attachments of selected types** option is enabled.

If the check box next to the file mask is selected, the Mail Threat Protection component renames or deletes files of this type when filtering email attachments.

If the check box next to the file mask is cleared, the Mail Threat Protection component 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 the Mail Threat Protection component.

The following setting is available:

File mask

The file mask input field, in accordance with which the Mail Threat Protection component filters attachments in email messages.

Additional tab

In this window, the administrator can configure the heuristic analysis settings for the Mail Threat Protection component.

The following settings are available:

Heuristic Analysis

This check box enables or disables the use of heuristic analysis when email is scanned by the Mail Threat Protection component.

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 scan** and **Medium scan** 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.

Application Control subsection

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

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

The following settings are available:

Application Control

This check box enables or disables the Application 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.

The check box is selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **Application Control Settings** section lets you create application control rules and select the Application Control mode.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

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 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 Control rule** window. You can create a new rule in this window.

Edit

Clicking this button opens the **Application 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.

Static analysis

This button opens the **Analysis of the access rights list** window. In this window, you can check whether the Application Control rules created in the current policy are working properly.

Application Control mode

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

You can choose one of the following items:

- **Black List**. If this item is selected, Application Control allows all users to start any applications, except in cases that satisfy the conditions of Application Control block rules.
- **White List**. If this item is selected, Application Control blocks all users from starting any applications, except in cases that satisfy the conditions of Application Control allow rules.

When **White list** mode is selected, two Application Control rules are automatically created:

- **Golden Image**.
- **Trusted Updaters**.

You cannot edit the settings of or delete automatically created rules. You can enable or disable these rules. By default, the **Golden Image** rule is enabled, and the **Trusted Updaters** rule is disabled.

The **Black List** item 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 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 Application Control mode, 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 an application that is blocked in the current Application Control mode, but logs information about its startup in the report.

The default option is **Block**.

Application Control rules

Table containing a list of Application Control rules.

The table contains the following columns:

- **Status**. This column displays the operating status of the rule. Left-clicking brings up a context menu in which you can select one of the following statuses:
  - **On**. This status means that the rule is used when the Application Control component is running.
  - **Off**. This status means that the rule is ignored when the Application Control component is running.
  - **Test**. This status means that Kaspersky Endpoint Security allows the startup of an application that is blocked in the current Application Control mode, but logs information about its startup in the report.

You can use the **Test** status to specify the **Notify** action for some of the rules if the **Block** option is selected in the **Action** drop-down list.

- **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.

Control 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.

When enabling the function for controlling which DLL modules and drivers are loaded, make sure that the Application Control section has enabled the default Golden Image rule or another rule that contains the Trusted certificates KL category and ensures that trusted DLL modules and drivers are loaded before Kaspersky Endpoint Security is started. Enabling control of the loading of DLL modules and drivers when the Golden Image rule is disabled may cause instability in the operating system.

Kaspersky Endpoint Security monitors only DLL modules and drivers that are loaded after the Control DLL and drivers check box was selected. It is recommended to restart the computer after selecting the Monitor DLLs and drivers check box in order for Kaspersky Endpoint Security to monitor all DLL modules and drivers, including those loaded before Kaspersky Endpoint Security starts.

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.

The **Advanced Settings** section lets you configure the templates for messages about blocking application startup and messages for the network administrator.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Templates

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

Blockage tab

The entry field contains the template of the message that is displayed when an Application 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 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 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 administrator.

Subject

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

The default subject is `[Application 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 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 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 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 Control rule window

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

An Application Control rule contains the KL category used to create the rule, and the action performed by the Application Control component when the rule is triggered (allowing or blocking application startup by users).

The administrator can perform the following actions on Application 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 Control rule is enabled by default after it is created.
- Delete rule

To work with Application 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 Control rule has been defined. You can leave this field empty.

Principals and their rights

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

The table contains the following columns:

- **Principal**. This column shows the users and/or user groups covered by the Application 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 **Principal** 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 **Principal** 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 **Users and / or groups that are granted permission** field from starting applications that match the rule.

If this check box is cleared, the application blocks only users that appear in the **Users and / or groups that are denied permission** field from starting applications that match the rule.

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.

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:

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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration

Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled / Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **Device Control Settings** section lets you create device access rules based on the type of device or connection bus, and create a list of trusted devices.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

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.

Login.

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.

Types of devices

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.
- **Access**. This column shows the status of access to the types of devices (*Allow*, *Block*, *Depends on bus, Restrict by rules*).

  A rule is assigned *Restrict by rules* access status if its status had been *Allow* and you have changed the rule settings.

Connection buses

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

The table contains the following columns:

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

Add

A button for adding devices to the Trusted list. Clicking this button opens a context menu with the following items:

- **Devices by ID**. Opens the **Add trusted devices by ID** window. This window lets you view a list of devices with known unique IDs and select devices that you want to add to the Trusted list.
- **Devices by model**. Opens the **Add trusted devices by model** window. This window lets you view a list of devices with known VID and PID parameters and select devices that you want to add to the Trusted list. The VID and PID settings identify the device model.
- **Devices by ID mask**. Opens the **Add trusted devices by ID mask** window. This window lets you enter the mask of a device ID based on which the application creates a rule for adding devices to the Trusted list.

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.

Import

Clicking this button imports a list of trusted devices from an XML file.

Export

Clicking this button exports the list of trusted devices or a subset of items in the list of trusted devices to an XML file.

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.

Anti-Bridging

Clicking this button opens the **Anti-Bridging** window. In this window, you can configure the Anti-Bridging settings.

The **Advanced Settings** section lets you configure the templates for messages about blocking access to a device and messages for the network administrator.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.

- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Templates

This button opens the **Message 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 network administrator.

Anti-Bridging window

Enable Anti-Bridging

This check box enables / disables Network Attack Blocker.

If the check box is selected, Kaspersky Endpoint Security blocks network bridges in accordance with the connection rules.

If the check box is cleared, Kaspersky Endpoint Security does not block network bridges.

This check box is cleared by default.

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.

The button is available if you have selected any item in the list of rules other than the top item.

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.

The button is available if you have selected any item in the list of rules other than the bottom item.

Rules for devices

Connection rules table. If the rule is used, Kaspersky Endpoint Security:

- Blocks the active connection when establishing a new connection, if the device type specified in the rule is used for both connections.
- Blocks connections established using the device types for which lower-priority rules

are used.

The table contains the following columns:

- **Control**. This column displays one of the following rule statuses:
  - *En.* The rule is used.
  - *Dis.* The rule is not used.
- **Device type**. This column displays the type of device used to established the connection. This column displays one of the following predefined types of devices:
  - Network adapter.
  - Wi-Fi.
  - Modem.

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 network 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 network 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 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 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.

- **Disabled**.

  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.

/Refresh

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 a particular 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.

/Refresh

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 a particular 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.

/Refresh

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 a particular 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 access 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 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:

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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On all client computers, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited from the Kaspersky Endpoint Security interface on client computers.

- Kaspersky Security Center blocks the enabling / disabling of the component in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of all these policies, the component operation status (*Enabled* / *Disabled*) is the same as the status that is defined in the top level policy properties.

> This block does not affect the capability to modify component settings if the component is enabled. If the component is enabled and the "lock" is open for one or several groups of its settings, the settings of these groups can be edited in the properties of policies that inherited top level policy settings.

The button with the open "lock" means the following:

- Kaspersky Security Center allows the enabling / disabling of the component from the Kaspersky Endpoint Security interface on client computers. On each client computer, the component is enabled or disabled according to the check box in the Kaspersky Endpoint Security local interface (selected or cleared).
- Kaspersky Security Center allows the enabling / disabling of the component in the properties of the policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. In the properties of each of these policies, the component operation status (*Enabled* / *Disabled*) does not depend on the status that is indicated in the top level policy settings.

The "lock" is closed by default.

The **Web Control Settings** section lets you generate rules for accessing web resources.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed 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.

The button is available if you have selected any item in the list of rules other than the top item.

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.

The button is available if you have selected any item in the list of rules other than the bottom item.

Search field

In the search field, you can enter the entire contents or any number of characters from the contents of the **Rule name** or **Users** columns of the web resources access rule that you want to find in the **Access rules sorted by priority** table.

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

Access rules

Table with list of web resource access rules. The access rules are sorted in the table based on their priority. The higher the rule priority, the higher its position in the table.

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. The rule covers those users.
- **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 it is not recommended to visit the web resources listed in the rule while in the corporate network.

The **Advanced Settings** section lets you configure the templates for messages about blocking web resources and messages to the local corporate network administrator.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Templates

This button opens the **Message 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 network 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 network administrator.

Subject

The message subject is entered in this field.

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 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 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 website (%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 (see section "Web resource content categories" on page 109) 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 for 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.

Rule schedule window

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 for 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 5), only full disk encryption using BitLocker Drive Encryption technology is available.

This section contains information about encryption and decryption of files on local computer drives, hard drives and removable 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

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 your 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:

- **File Level Encryption 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.

For details on applying a Kaspersky Security Center policy, please refer to the Kaspersky Security Center Help Guide.

- **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.
- **Full Disk Encryption**. 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 full disk encryption rule and create a list of hard drives to be excluded from encryption. Kaspersky Endpoint Security performs full disk encryption by sector after the Kaspersky Security Center policy is applied. The application encrypts all logical partitions of hard drives simultaneously. For details on applying a Kaspersky Security Center policy, please refer to the Kaspersky Security Center Help Guide.

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 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 Help Guide.

> When the application version is upgraded to Kaspersky Endpoint Security 11 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 full disk encryption functionality (see section "Working with encrypted devices when there is no access to them" on page 158). 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 used disk space only** function enabled 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 network administrator;
- restore 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 0.5% 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 the 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 159

Restoring data on encrypted devices using the Restore Utility 161

Common encryption settings section

If the "lock" is open, the settings corresponding to this lock will not be applied on the client computer that has Kaspersky Endpoint Security installed.

Safely delete original files after encryption is complete

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 selected by default.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to this setting in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The value of this setting that is defined in top level policy properties is used.

The button with the open "lock" means that Kaspersky Security Center allows changes to this setting in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The value of this setting does not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

The **Password settings** section lets you configure passwords for Authentication Agent, Portable File Manager, and encrypted archives.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

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.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

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 must enter the operating system user account credentials for accessing encrypted hard drives and then automatically logging into the operating system.

If the check box is cleared, to access encrypted hard drives and subsequently automatically log into the operating system you must separately enter the credentials for accessing encrypted drives and the operating system user account credentials.

When using Single Sign-On (SSO) technology, all settings on the Authentication Agent tab are unavailable except the **Block password after N failed input attempt(s)** setting.

This check box is selected by default.

Minimum password length

Field for specifying minimum password length in characters.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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 available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and the **Assess password strength** check box is selected.

This check box is selected by default.

Block reuse of the previous password

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 available if the **Use Single Sign-On (SSO) technology** check box is cleared.

This check box is selected 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.

If the check box is cleared, the password is valid for an unlimited amount of time.

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.

If the check box is cleared, there is no limit on the number of allowed attempts to enter the password.

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 network 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 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 administrator.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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 characters.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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 available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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 characters.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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 available if the **Use Single Sign-On (SSO) technology** check box is cleared.

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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and 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.

This check box is available if the **Use Single Sign-On (SSO) technology** check box is cleared and the **Assess password strength** check box is selected.

This check box is selected by default.

Block reuse of the previous password

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 available if the **Use Single Sign-On (SSO) technology** check box is cleared.

This check box is selected 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.

If the check box is cleared, the password is valid for an unlimited amount of time.

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.

User message tab

To

Field for entering the email address of the network administrator.

Subject

Field for entering the subject of the email message used to request access to encrypted files.

The subject `Request for access to encrypted files` is entered by default.

Entry field

This field shows the text of the email message template. Clicking the **Send by email** button in the **File access denied** window automatically creates a message. The **File access denied** window opens when the user attempts to access an encrypted file on a computer without a key for transparent access to encrypted files.

You can edit the message 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%)**. The variable is replaced with the name of the current account of the user who is requesting access to encrypted files.
- **Computer name (%COMPUTER_NAME%)**. The variable is replaced with the name of the computer that stores the encrypted files to which the user is requesting access.
- **Device type (%DEVICE_TYPE%)**. The variable is replaced with the name of the type of device that stores the encrypted files to which the user is requesting access.
- **Current date (%DATE%)**. The variable is replaced with the date of the user request for access to encrypted files.
- **Current time (%TIME%)**. The variable is replaced with the time of the user request for access to encrypted files.

Administrator message tab

Entry field

This field shows the text of the email message template. Clicking the **Send by email** button in the **File access denied** window automatically creates a message. The **File access denied** window opens when the user attempts to access an encrypted file on a computer without a key for transparent access to encrypted files.

You can edit the message 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%)**. The variable is replaced with the name of the current account of the user who is requesting access to encrypted files.

- **Computer name (%COMPUTER_NAME%)**. The variable is replaced with the name of the computer that stores the encrypted files to which the user is requesting access.
- **Device type (%DEVICE_TYPE%)**. The variable is replaced with the name of the type of device that stores the encrypted files to which the user is requesting access.
- **Current date (%DATE%)**. The variable is replaced with the date of the user request for access to encrypted files.
- **Current time (%TIME%)**. The variable is replaced with the time of the user request for access to encrypted files.

Authentication tab

Entry field

This field shows the template of help text that appears when an account name and password are entered in the Authentication Agent.

You can edit the help text template.

> You can enter help text containing 16 lines or less. The maximum length of a line is 64 characters.
> Before editing help messages of the Authentication Agent, please review the list of supported characters in the preboot environment. This list can be found in the Online Help resource at the following link: https://stage.help.kaspersky.com/KESWin/11/en-US/132151.htm

By default

This button restores the original text of the template. This button is available if you have changed the text of the template.

Password change tab

Entry field

This field shows the template of help text that appears when changing an account password in the Authentication Agent.

You can edit the help text template.

> You can enter help text containing 16 lines or less. The maximum length of a line is 64 characters.
> Before editing help messages of the Authentication Agent, please review the list of supported characters in the preboot environment. This list can be found in the Online Help resource at the following link: https://stage.help.kaspersky.com/KESWin/11/en-US/132151.htm

By default

This button restores the original text of the template. This button is available if you have changed the text of the template.

Password recovery tab

Entry field

This field shows the template of help text that appears during account password recovery in the Authentication Agent.

You can edit the help text template.

> You can enter help text containing 16 lines or less. The maximum length of a line is 64 characters.
> Before editing help messages of the Authentication Agent, please review the list of supported characters in the preboot environment. This list can be found in the Online Help resource at the following link: https://stage.help.kaspersky.com/KESWin/11/en-US/132151.htm

By default

This button restores the original text of the template. This button is available if you have changed the text of the template.

Full Disk Encryption

> If Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for Workstations, BitLocker Drive Encryption and Kaspersky Disk Encryption technologies are available for encryption. If Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for file servers (see section "Hardware and software requirements" on page 5), only BitLocker Drive Encryption technology is available.

This section contains information on full disk encryption and instructions on configuring and performing full disk encryption with Kaspersky Endpoint Security and the Kaspersky Endpoint Security administration plug-in.

In this section:

About Full Disk Encryption

Before starting full disk encryption, the application runs a series of checks to determine if the device can be encrypted, which includes checking the system hard drive for compatibility with Authentication Agent or 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, full disk encryption starts after the operating system has loaded and the 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 full disk encryption 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, prior to full disk 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 full disk 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 full disk encryption, Authentication Agent is loaded before the next startup of the operating system. Kaspersky Endpoint Security resumes full disk encryption after successful authentication in Authentication Agent and operating system startup.

If the operating system switches to hibernation mode during full disk encryption, Authentication Agent is loaded when the operating system switches back from hibernation mode. Kaspersky Endpoint Security resumes full disk encryption after successful authentication in Authentication Agent and operating system startup.

If the operating system goes into sleep mode during full disk encryption, Kaspersky Endpoint Security resumes full disk encryption 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 network administrator using Kaspersky Security Center tools.
- Enter the password of a token or smart card connected to the computer.

> Use of a token or smart card is available only if the computer hard drives were encrypted using the AES256 encryption algorithm. If the computer hard drives were encrypted using the AES56 encryption algorithm, addition of the electronic certificate file to the command will be denied.

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 161), 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

Full Disk Encryption 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 full disk encryption.

The drop-down list contains the following items:

- **Not specified**. If this item is selected, the application does not perform full disk encryption 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 for full disk encryption when the Kaspersky Security Center policy is applied.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks the selection of items from this list and blocks changes to settings associated with this list in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows the selection of items from this list and blocks changes to settings associated with this list in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

If the "lock" is open, the settings defined in the policy will not be applied on the client computer with Kaspersky Endpoint Security installed.

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.

If the computer has several operating systems installed, after encryption you will be able to load only the operating system that has the application installed.

- **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 hard drives in their previous state when the Kaspersky Security Center policy is applied. If the hard drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted.

The **Leave unchanged** item is selected by default.

Automatically create Authentication Agent accounts for users

This check box enables / disables automatic creation of Authentication Agent accounts when applying a policy.

If the check box is selected, when a policy is applied, Kaspersky Endpoint Security creates those Authentication Agent accounts not created previously according to the settings specified in the **Authentication Agent account creation settings** window. The **Authentication Agent account creation settings** window is opened by clicking the link on the word *users*.

If the check box is cleared, when a policy is applied, Kaspersky Endpoint Security does not create Authentication Agent accounts, and the settings specified in the **Authentication Agent account creation settings** window are ignored.

To view a list of Authentication Agent accounts, open the properties of the local *Encryption (account management)* task.

This check box is selected 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 option that limits the encryption area to only occupied hard drive sectors. This limit lets you reduce encryption time.

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.

If the check box is selected, only portions of the hard 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 hard drive is encrypted, including residual fragments of previously deleted and modified files.

This option is recommended for new hard drives whose data has not been modified or deleted. If you are applying encryption on a hard drive that is already in use, it is recommended to encrypt the entire hard drive. This ensures protection of all data, even deleted data that is potentially recoverable.

This check box is cleared by default.

Use Legacy USB Support (not recommended)

This check box enables / disables the Legacy USB Support option that is responsible for supporting USB devices during initial startup of the computer. Enabling / disabling this option does not affect support for USB devices after the operating system is started.

If the check box is selected, support for USB devices during initial startup of the computer will be enabled.

Enabling Legacy USB Support reduces the security level of the computer during initial startup of the computer. It is recommended to use this option only when there is a hardware compatibility issue and only for those computers on which the problem occurred.

If the check box is cleared, support for USB devices during initial startup of the computer will be disabled.

This check box is cleared by default.

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 hard 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.

If the computer has several operating systems installed, after encryption you will be able to load only the operating system that has the application installed.

- **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 hard drives in their previous state when the Kaspersky Security Center policy is applied. If the hard drive was encrypted, it remains encrypted. If the drive was decrypted, it remains decrypted.

The **Leave unchanged** 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 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 option that limits the encryption area to only occupied hard drive sectors. This limit lets you reduce encryption time.

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.

If the check box is selected, only portions of the hard 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 hard drive is encrypted, including residual fragments of previously deleted and modified files.

This option is recommended for new hard drives whose data has not been modified or deleted. If you are applying encryption on a hard drive that is already in use, it is recommended to encrypt the entire hard drive. This ensures protection of all data, even deleted data that is potentially recoverable.

This check box is cleared by default.

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 value in the field cannot be less than six.

The minimum PIN length is six 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.

/Refresh

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 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.

Authentication Agent account creation settings window

All accounts on the computer

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for all computer accounts that have ever been active.

This check box is selected by default.

All domain accounts on the computer

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for all computer accounts belonging to a certain domain that have ever been active.

This check box is cleared by default.

All local accounts on the computer

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for all local computer accounts that have ever been active.

This check box is cleared by default.

Active for N days

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates Authentication Agent accounts for the selected accounts that have been active on the computer during the past N days.

The default value is set to 30 days.

Local administrator

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates a local administrator account.

This check box is selected by default.

Computer manager

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security creates an Authentication Agent account for the account whose properties in Active Directory show that it is a management account.

This check box is cleared by default.

Active account

If this check box is selected, when running the full disk encryption task Kaspersky Endpoint Security automatically creates an Authentication Agent account for the computer account that is active during the task.

This check box is cleared by default.

File Level Encryption on local computer drives

File Level Encryption on local computer drives is available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for workstations. File Level Encryption on local computer drives 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 5).

This section covers encryption of files on local computer drives and provides instructions on how to configure and perform encryption of files on local computer drives with Kaspersky Endpoint Security and the Kaspersky Endpoint Security Console Plug-in.

In this section:

File Level Encryption section

If the "lock" is open, the settings corresponding to this lock will not be applied on the client computer that has Kaspersky Endpoint Security installed.

Encryption mode

Drop-down list whose items determine the action that Kaspersky Endpoint Security performs on files and folders on local drives of the computer.

The drop-down list contains the following items:

- **Leave unchanged**. If this item is selected, Kaspersky Endpoint Security leaves the files and folders unchanged without encrypting or decrypting them.
- **Default rules**. If this item is selected, Kaspersky Endpoint Security encrypts the files and folders specified on the **Encryption** tab, decrypts the files and folders specified on the **Decryption** tab, and regulates the access of applications to encrypted files according to the rules specified on the **Rules for applications** tab.
- **Decrypt all files**. If this item is selected, Kaspersky Endpoint Security decrypts all encrypted files and folders.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks the selection of items from this list and blocks changes to settings associated with this list in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows the selection of items from this list and blocks changes to settings associated with this list in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Encryption

This tab shows encryption rules for files stored on local drives.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to this tab's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows changes to this tab's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Add

Clicking this button opens the button context menu with the following items:

- **Predefined folders**. Selecting this item opens the **Select predefined folders** window. This window allows selecting folders suggested by Kaspersky Lab specialists for addition to the encryption list.
- **Custom folder**. Selecting this item opens the **Add custom folder** window. This window lets you type the path to a folder that you want to add to the encryption list.
- **Files by extension**. Selecting this item opens the **Add / edit list of file extensions** window. This window allows creating a list of file extensions that you want to add to the encryption list.
- **Files by group(s) of extensions**. Selecting this item opens the **Select groups of file extensions** window. This window allows selecting groups of file extensions that you want to add to the encryption list.

Edit

Clicking this button opens a window. You can edit a file encryption rule in this window.

This button is available when a file encryption rule is selected in the table.

Delete

Clicking this button opens the button context menu with the following items:

- **Delete rule**. If this item is selected, Kaspersky Endpoint Security deletes the file encryption rule selected in the table.
- **Delete rule and decrypt files**. If this item is selected, Kaspersky Endpoint Security deletes the file encryption rule selected in the table and decrypts the files specified in the rule the next time the Kaspersky Security Center policy is applied.

This button is available when a file encryption rule is selected in the table.

Decryption

This tab shows decryption rules for files stored on local drives.

Buttons 🔒 **and** 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to this tab's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows changes to this tab's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Add

Clicking this button opens the button context menu with the following items:

- **Predefined folders**. Selecting this item opens the **Select predefined folders** window. This window allows selecting folders suggested by Kaspersky Lab specialists for addition to the decryption list.
- **Custom folder**. Selecting this item opens the **Add custom folder** window. This window lets you type the path to a folder that you want to add to the decryption list.
- **Files by extension**. Selecting this item opens the **Add / edit list of file extensions**

window. This window allows creating a list of file extensions that you want to add to the decryption list.

- **Files by group(s) of extensions**. Selecting this item opens the **Select groups of file extensions** window. This window allows selecting groups of file extensions that you want to add to the decryption list.

Edit

Clicking this button opens a window. You can edit a file decryption rule in this window.

This button is available when a file decryption rule is selected in the table.

Delete

Clicking this button deletes the object selected from the encryption list.

This button is available if an encrypted object is selected.

Rules for applications

The tab displays a table containing encrypted file access rules for applications and encryption rules for files that are created or modified by individual applications.

The table contains the following columns:

Application / List of applications. Column that displays the name or a list of names of executable files of applications. These applications are subject to an encrypted file access rule or an encryption rule for files that are created or modified by applications.

- **Rule**. This column shows a rule. This rule defines the access of an application or group of applications to encrypted files, or the encryption of files that are created or modified by applications.

Buttons 🔒 **and** 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to this tab's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows changes to this tab's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Add

Clicking this button opens the button context menu with the following items:

- **Applications from Kaspersky Security Center list**. Selecting this item opens the **Add applications from Kaspersky Security Center list** window. This window lets you select applications for which you want to define rules for accessing encrypted files or rules for encrypting files that are created or modified by applications.
- **Custom applications**. Selecting this item opens the **Add / edit names of the executable files of applications** window. This window lets you manually enter the names of executable files of applications for which you want to define rules for accessing encrypted files or rules for encrypting files that are created or modified by applications.

Edit

Clicking this button opens the **Add / edit names of the executable files of applications** window. This window lets you edit the names of executable files of applications for which you want to define rules for accessing encrypted files or rules for encrypting files that are created or modified by applications.

This button is available when an entry is selected in the table.

Delete

Clicking this button removes the entry corresponding to an application or group of applications from the table.

This button is available when an entry is selected in the table.

Search field

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

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

Select predefined folders window

List of predefined folders

This list contains local user account folders that Kaspersky Lab specialists recommend for encryption:

- **My Documents**. User files are stored in this folder by default.
- **Favorites**. This folder stores bookmarks of the Internet Explorer browser.
- **Desktop**. This folder contains desktop items, including user files and folders.
- **Temporary files**. This folder stores temporary files and folders of applications that are running under the user account.
- **Outlook files**. This folder stores personal folder files (*.pst), offline folder files (*.ost), offline address book files (*.oab), personal address book files (*.pab), signature files (*.rtf, *.txt, *.htm), and temporary message files (OLK).

The check box opposite the folder name includes the folder in the list of objects or excludes it.

If the check box opposite the folder name is selected, the folder is included in the list of objects.

Add custom folder window

Entry field

Field for typing the path to a folder that you want to add to the list of objects.

You can use environment variables. For example: `%ALLUSERSPROFILE%\Desktop`.

Add / edit list of file extensions window

Entry field

Field for entering or editing the list of file extensions. The list of file extensions is included in the list of objects.

Select groups of file extensions window

Add

Clicking this button opens the **Add / edit a group of file extensions** window. This window lets you create a new group of file extensions.

Edit

Clicking this button opens the **Add / edit a group of file extensions** window. This window lets you edit an existing group of file extensions.

This button is available if an item is selected in the list of file extension groups.

Delete

Clicking this button deletes the group of file extensions that is selected in the list of file extension groups.

This button is available if an item is selected in the list of file extension groups.

List of file extension groups

The check box opposite the name of a group of file extensions includes this group of file extensions in the list or excludes it.

If the check box opposite the name of a group of file extensions is selected, the group of file extensions is included in the list of objects.

Add / edit a group of file extensions window

Group name

Field for typing or editing the name of a group of file extensions.

Entry field

Field for typing a list of file extensions that you want to include in this group of file extensions.

Add applications from the Kaspersky Security Center list window

Application

Field for entering the name of an application. You can use this name to filter the consolidated list of all applications that are installed on computers that are subject to the policy.

You can enter any number of characters from the application name.

Vendor

This field is used to enter the name of the application vendor. You can use this name to filter the consolidated list of all applications that are installed on computers that are subject to the policy.

You can enter any number of characters from the application vendor name.

Group

List of trust groups. The check box next to the name of a trust group enables / disables filtering of the consolidated list of all applications that are installed on computers that are subject to the policy by trust group name.

When one or more check boxes next to the names of trust groups are selected, the table lists the applications that belong to the corresponding trust groups.

When all check boxes next to the names of trust groups are cleared, filtering of the consolidated list of all applications that are installed on computers that are subject to the policy by trust group name is disabled. The table lists applications whose parameters match the remaining specified filters.

All check boxes are selected by default.

Period added

A drop-down list whose items let you specify a filter by the period of time when applications that are installed on computers that are subject to the policy were added to the consolidated list of applications by using the inventory task. Possible drop-down list items:

- **Last 24 hours**. When this item is selected, the table lists applications that have been added to the consolidated list of applications in the last 24 hours.
- **Last week**. When this item is selected, the table lists applications that have been added to the consolidated list of applications in the last 7 days.
- **Last month**. When this item is selected, the table lists applications that have been added to the consolidated list of applications during the last month.
- **Last year**. When this item is selected, the table lists applications that have been added to the consolidated list of applications during the last full year.
- **All time**. When this item is selected, the table lists applications that have been added to the consolidated list of applications since the inventory task was first started.
- **Custom**. When this item is selected, the table lists applications that have been added to the consolidated list of applications during the period whose start and end dates are specified in the **from** and **to** fields.

from

Field for entering the start of the period during which applications were added to the consolidated list of all applications that are installed on computers that are subject to the policy.

This field is available when the item that is selected in the **Period added** drop-down list is **Custom**.

to

Field for entering the end of the period during which applications were added to the consolidated list of all applications that are installed on computers that are subject to the policy.

This field is available when the item that is selected in the **Period added** drop-down list is **Custom**.

/Refresh

Clicking this button causes the specified filters to be applied to the consolidated list of all applications that are installed on computers that are subject to the policy.

Select all

Clicking this button selects check boxes in the **Application** column opposite the names of all applications in the table.

Deselect

Clicking this button clears check boxes in the **Application** column opposite the names of all applications in the table.

Application

This column shows the application name.

File version

This field shows the version of the executable file of the application.

Vendor

This column shows the name of the application vendor.

Group

This field shows the name of the trust group to which Kaspersky Endpoint Security assigns the application.

Date of update

This column shows the date when the application was added to the specified trust group.

Rule for application(s)

A drop-down list containing items that define the encrypted file access rule for applications and the action to be taken by Kaspersky Endpoint Security on files that are created by applications. Possible drop-down list items:

- **Encrypt all created files**. If this option is selected, Kaspersky Endpoint Security encrypts all files that are created by applications specified in the list above.
- **Block access to encrypted files**. If this option is selected, Kaspersky Endpoint Security restricts applications specified in the list above from accessing encrypted files.
- **Grant access to encrypted files in ciphertext only**. If this option is selected, Kaspersky Endpoint Security allows the applications specified in the list above to access encrypted files as ciphertext only.

Actions for applications that were selected earlier

A drop-down list containing items that define the action. Kaspersky Endpoint Security takes this action on rules of application access to encrypted files. Possible drop-down list items:

- Updater If this option is selected, Kaspersky Endpoint Security updates the encrypted file access rule for previously selected applications for which the encrypted file access rule has been configured, and does so according to the value that is selected in the **Rule for application(s)** drop-down list.
- **Skip**. If this option is selected, Kaspersky Endpoint Security does not modify the encrypted file access rule for previously selected applications for which the encrypted file access rule has been configured.

Add / edit names of the executable files of applications window

Entry field

Field for typing the name or list of names of executable files of applications that are restricted from accessing encrypted files.

Add from Kaspersky Security Center list

Clicking this button opens the **Add applications from Kaspersky Security Center list** window. This window lets you select applications to be added to the list of applications that are restricted from accessing encrypted data. This window shows a Kaspersky Security Center-consolidated list of all applications installed on computers that are subject to the Kaspersky Security Center policy.

Description

Field for typing the details of the list of applications that are restricted from accessing encrypted files.

Rule for application(s)

A drop-down list containing items that define the encrypted file access rule for applications and the action to be taken by Kaspersky Endpoint Security on files that are created by applications. Possible drop-down list items:

- **Encrypt all created files**. If this option is selected, Kaspersky Endpoint Security encrypts all files that are created by applications specified in the list above.
- **Block access to encrypted files**. If this option is selected, Kaspersky Endpoint Security restricts applications specified in the list above from accessing encrypted files.
- **Grant access to encrypted files in ciphertext only**. If this option is selected, Kaspersky Endpoint Security allows the applications specified in the list above to access encrypted files as ciphertext only.

Encryption of removable drives

Encryption of removable drives is available if Kaspersky Endpoint Security is installed on a computer running Microsoft Windows for workstations. Encryption of removable drives 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 5).

This section contains information on encryption of removable drives and instructions on configuring and performing encryption of removable drives using Kaspersky Endpoint Security and the Kaspersky Endpoint Security administration plug-in.

In this section:

Encryption of removable drives section

If the "lock" is open, the settings corresponding to this lock will not be applied on the client computer that has Kaspersky Endpoint Security installed.

Encryption mode

Drop-down list whose items determine the action that Kaspersky Endpoint Security performs on the files on removable drives.

The drop-down list contains the following items:

- **Encrypt entire removable drive**. If this item is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts removable drives sector by sector, including their file systems.
- **Encrypt all files**. If this item is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts all files that are stored on removable drives. Kaspersky Endpoint Security does not encrypt already-encrypted files again. The contents of the file system of removable drives, including the names of encrypted files and folder structure, are not encrypted and remain accessible.
- **Encrypt new files only**. If this item is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts only those files that were added or modified on the removable drives after the Kaspersky Security Center policy was last applied.

  This encryption mode is convenient when a removable drive is used for both personal and work purposes. This encryption mode lets you leave all old files unchanged and encrypt only those files that the user creates on a work computer that has Kaspersky Endpoint Security installed and encryption functionality enabled. As a result, access to personal files is always available, regardless of whether or not Kaspersky Endpoint Security is installed on the computer with encryption functionality enabled.
- **Decrypt entire removable drive**. If this item is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security decrypts all encrypted files stored on removable drives as well as the file systems of the removable drives if they were previously encrypted.
- **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.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks the selection of items from this list and blocks changes to settings associated with this list in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows the selection of items from this list and blocks changes to settings associated with this list in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Portable mode

This check box is available if **Encrypt all files** or **Encrypt new files only** is selected in the **Encryption mode** drop-down list.

This check box enables / disables the preparation of a removable drive that makes it possible to access files stored on this removable drive on computers without Kaspersky Endpoint Security encryption functionality.

If this check box is selected, Kaspersky Endpoint Security prompts the user to specify a password before encrypting files on a removable drive upon the application of the Kaspersky Security Center policy. The password is needed to access files encrypted on a removable drive on computers without Kaspersky Endpoint Security encryption functionality. You can configure the password settings in the Kaspersky Security Center policy properties in the **Data encryption** section in the **Common encryption settings** subsection.

This check box is cleared by default.

Encrypt used disk space only

This check box enables / disables the encryption mode in which only occupied disk sectors 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.

This check box is available if the **Encrypt entire removable drive** option is selected in the **Encryption mode** drop-down list.

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.

Custom rules

This table contains devices for which custom encryption rules are defined.

The table contains the following columns:

- **Device**. This column shows the names of removable drives for which encryption rules have been defined.
- **Device ID**. This column shows the IDs of removable drives for which encryption rules have been defined.
- **Rule**. This column shows an action. This action is performed by Kaspersky Endpoint Security on an attempt to access a removable drive for which an encryption rule has been defined.
- **Portable mode**. This column shows information about the capability of a removable drive to access its stored encrypted files on computers that do not have Kaspersky Endpoint Security encryption functionality.
- **Encrypt used disk space only**. This column displays information about whether Kaspersky Endpoint Security encrypts only those sectors that are occupied by files or encrypts all sectors of the removable drive.

Buttons 🔒 and 🔓

The button with the closed "lock" means that Kaspersky Security Center blocks changes to this table's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means that Kaspersky Security Center allows changes to this table's settings in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Add

Clicking this button opens the button context menu with the following items:

- **From list of trusted devices of this policy**. Selecting this item opens the **Add devices from the list of trusted devices** window. This window lets you select the device for whose files you want to specify an encryption rule.
- **From Kaspersky Security Center list of devices**. Selecting this item opens the **Add devices from Kaspersky Security Center list** window. This window lets you select the device for whose files you want to specify an encryption rule.

Set a rule

Clicking this button opens a drop-down list with the following items:

- **Leave unchanged**. If this option is selected, when files on the device that is selected in the table are accessed, Kaspersky Endpoint Security leaves the files in their previous state. If the file was encrypted, it remains encrypted. If the file was decrypted, it remains decrypted.
- **Encrypt new files only**. If this option is selected, when files on the device that is selected in the table are accessed, Kaspersky Endpoint Security encrypts only files that have been added or modified after the Kaspersky Security Center policy was last applied.

  This encryption rule is convenient when a removable drive is used for both personal and work purposes. This encryption rule lets you keep all old files unchanged and encrypt only those files that the user creates on a work computer that has Kaspersky Endpoint Security installed and encryption functionality enabled. As a result, access to personal files is always available, regardless of whether or not Kaspersky Endpoint

Security is installed on the computer with encryption functionality enabled.

- **Encrypt all files**. If this option is selected, when an attempt is made to access a device that is selected in the table, Kaspersky Endpoint Security encrypts all files stored on it.

  Kaspersky Endpoint Security does not encrypt already-encrypted files again.
- **Decrypt entire removable drive**. If this option is selected, when an attempt is made to access a removable drive that is selected in the table, Kaspersky Endpoint Security decrypts all encrypted files that are stored on it, as well as the file system of the removable drive if it was encrypted.
- **Encrypt entire removable drive**. If this item is selected, when an attempt is made to access a device that is selected in the table, Kaspersky Endpoint Security encrypts removable drives sector by sector, including their file systems.
- **Encrypt used disk space only**. If this item is selected, when an attempt is made to access a device that is selected in the table, Kaspersky Endpoint Security encrypts only those sectors that are occupied by files.

This button lets you edit encryption rules of removable drives selected in the **Custom rules** table.

The button is unavailable if no removable drive is selected in the **Custom rules** table.

Delete

Clicking this button deletes the encryption rule for the device selected from the table.

This button is available when an entry is selected in the table.

Search field

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

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

Allow removable drive encryption in offline mode

If this check box is selected, Kaspersky Endpoint Security encrypts removable drives even when there is no connection to Kaspersky Security Center. In this case, the data required for decrypting removable drives is stored on the hard drive of the computer to which the removable drive is connected, and is not transmitted to Kaspersky Security Center.

If the check box is cleared, Kaspersky Endpoint Security does not encrypt removable drives without a connection to Kaspersky Security Center.

This check box is cleared by default.

Add devices from Kaspersky Security Center list window

Display devices in the table for which the following is defined

A drop-down list whose items set a filter for the consolidated list of all devices that have been connected to computers that are subject to the policy:

- **Device model**. If this option is selected, the table displays only devices with known VID and PID parameters. The VID and PID settings identify the device model.
- **Device ID**. If this option is selected, the table displays only devices with known unique IDs.

Name

A field for entering the name of the removable drive. The removable drive with the specified name is displayed in the table.

You can use the following special characters to define the name mask:

- `*` replaces any sequence of characters;
- `?` – any single character.

Computer

Field for entering the name of a computer. If the name of a computer is entered, the table with the list of devices displays the devices connected to this computer.

You can use the following special characters to define the name mask:

- `*` replaces any sequence of characters;
- `?` – any single character.

/Refresh

Clicking this button causes the table to display the devices according to the defined filter or based on the values defined in the **Name** and **Computer** fields.

Kaspersky Disk Encryption

A drop-down list that lets you specify a filter for displaying a list of devices that have been connected to computers subject to the policy, depending on whether or not the encryption operation is available for them:

- **Not considered**. If this option is selected, the table shows all devices.
- **Available**. If this item is selected, the table shows devices for which the encryption operation is available.
- **Not available**. If this item is selected, the table shows devices for which the encryption operation is unavailable.

Select all

Clicking this button selects check boxes in the **Device type** column opposite the names of all device types in the table.

Deselect

Clicking this button clears check boxes in the **Device type** column opposite the names of all device types in the table.

Devices that can be encrypted

This table displays the devices connected to client computers. You can define encryption rules for these devices.

If the check box in the line containing the removable drive is selected, Kaspersky Endpoint Security adds this removable drive to the encryption rule.

If the check box in the line containing the removable drive is cleared, Kaspersky Endpoint Security does not add this removable drive to the encryption rule.

The table contains the following columns:

- **Device type**. This column displays the type of device.
- **Name**. This column displays the device name.
- **Device model / ID**. This column displays the model or unique ID of the device.
- **Computer**. This column shows the name of the computer to which the device is connected.
- **Kaspersky Disk Encryption**. This column displays information about whether or not

Kaspersky Disk Encryption technology is available for the removable drive.

The availability of BitLocker Drive Encryption does not depend on the value specified in this column.

Encryption mode for selected devices

This drop-down list lets you select the action which Kaspersky Endpoint Security should perform on files stored on removable drives:

- **Encrypt entire removable drive**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts removable drives, including their file systems, sector by sector.
- **Encrypt all files**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts all files stored on removable drives. Kaspersky Endpoint Security does not encrypt already-encrypted files again. The contents of the file system of removable drives, including the names of encrypted files and folder structure, are not encrypted and remain accessible.
- **Encrypt new files only**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts only those files that have been added to removable drives or were stored on removable drives and have been modified after the Kaspersky Security Center policy was applied last.

  This encryption rule is convenient when a removable drive is used for both personal and work purposes. This encryption rule lets you keep all old files unchanged and encrypt only those files that the user creates on a work computer that has Kaspersky Endpoint Security installed and encryption functionality enabled. As a result, access to personal files is always available, regardless of whether or not Kaspersky Endpoint Security is installed on the computer with encryption functionality enabled.
- **Decrypt entire removable drive**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security decrypts all encrypted files stored on removable drives as well as the file systems of the removable drives if they were previously encrypted.
- **Leave unchanged**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security does not encrypt or decrypt files on removable drives.

Portable mode

This check box enables / disables the preparation of a removable drive that makes it possible to access files encrypted on the drive on computers without Kaspersky Endpoint Security encryption functionality.

If this check box is selected, Kaspersky Endpoint Security prompts the user to specify a password before encrypting the removable drive upon the application of the Kaspersky Security Center policy. The password is needed to access files encrypted on a removable drive on computers without Kaspersky Endpoint Security encryption functionality.

This check box is available if **Encrypt all files** or **Encrypt new files only** is selected in the **Encryption mode for selected devices** drop-down list.

This check box is cleared by default.

Encrypt used disk space only

This check box enables / disables the encryption mode in which only occupied disk sectors 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.

This check box is available if the **Encrypt entire removable drive** option is selected in the **Encryption mode** drop-down list.

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.

Actions for devices that were selected earlier

A drop-down list containing items that define the action. Kaspersky Endpoint Security takes this action on files stored on devices for which an encryption rule has been already defined. Possible drop-down list items:

- Updater If this option is selected, Kaspersky Endpoint Security updates the encryption rule for files on previously selected devices for which an encryption rule has been configured, and does so according to the value that is selected in the **Encryption mode for selected devices** drop-down list.
- **Skip**. If this option is selected, Kaspersky Endpoint Security does not modify the encryption rule for files on previously selected devices for which an encryption rule has been configured.

Add devices from the list of trusted devices window

Select all

Clicking this button selects check boxes in the **Device type** column opposite the names of all device types in the table.

Deselect

Clicking this button clears check boxes in the **Device type** column opposite the names of all device types in the table.

Search field

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

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

List of devices that can be encrypted

This table displays the devices connected to client computers. You can define encryption rules for these devices.

The table contains the following columns:

- **Device type**. This column displays the type of device.
- **Name**. This column displays the device name.
- **Device model / ID**. This column displays the model or unique ID of the device.
- **Users**. This column shows the names of users and / or user groups. These users

and / or user groups are granted full access (read and write) to the device.

Encryption mode for selected devices

This drop-down list lets you select the action which Kaspersky Endpoint Security should perform on files stored on removable drives:

- **Encrypt entire removable drive**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts removable drives, including their file systems, sector by sector.
- **Encrypt all files**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts all files stored on removable drives. Kaspersky Endpoint Security does not encrypt already-encrypted files again. The contents of the file system of removable drives, including the names of encrypted files and folder structure, are not encrypted and remain accessible.
- **Encrypt new files only**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security encrypts only those files that have been added to removable drives or were stored on removable drives and have been modified after the Kaspersky Security Center policy was applied last.

  This encryption rule is convenient when a removable drive is used for both personal and work purposes. This encryption rule lets you keep all old files unchanged and encrypt only those files that the user creates on a work computer that has Kaspersky Endpoint Security installed and encryption functionality enabled. As a result, access to personal files is always available, regardless of whether or not Kaspersky Endpoint Security is installed on the computer with encryption functionality enabled.
- **Decrypt entire removable drive**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security decrypts all encrypted files stored on removable drives as well as the file systems of the removable drives if they were previously encrypted.
- **Leave unchanged**. If this option is selected, when applying the Kaspersky Security Center policy with the specified encryption settings for removable drives, Kaspersky Endpoint Security does not encrypt or decrypt files on removable drives.

Portable mode

This check box enables / disables the preparation of a removable drive that makes it possible to access files encrypted on the drive on computers without Kaspersky Endpoint Security encryption functionality.

If this check box is selected, Kaspersky Endpoint Security prompts the user to specify a password before encrypting the removable drive upon the application of the Kaspersky Security Center policy. The password is needed to access files encrypted on a removable drive on computers without Kaspersky Endpoint Security encryption functionality.

This check box is available if **Encrypt all files** or **Encrypt new files only** is selected in the **Encryption mode for selected devices** drop-down list.

This check box is cleared by default.

Encrypt used disk space only

This check box enables / disables the encryption mode in which only occupied disk sectors 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.

This check box is available if the **Encrypt entire removable drive** option is selected in the **Encryption mode** drop-down list.

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.

Actions for devices that were selected earlier

A drop-down list containing items that define the action. Kaspersky Endpoint Security takes this action on files stored on devices for which an encryption rule has been already defined. Possible drop-down list items:

- Updater If this option is selected, Kaspersky Endpoint Security updates the encryption rule for files on previously selected devices for which an encryption rule has been configured, and does so according to the value that is selected in the **Encryption mode for selected devices** drop-down list.
- **Skip**. If this option is selected, Kaspersky Endpoint Security does not modify the encryption rule for files on previously selected devices for which an encryption rule has been configured.

Viewing data encryption details

This section describes how you can view the details of data encryption.

In this section:

About encryption status

While encryption or decryption in progress, Kaspersky Endpoint Security relays information about the status of encryption parameters applied to client computers to Kaspersky Security Center.

The following encryption status values are possible:

- *Encryption policy not defined*. A Kaspersky Security Center encryption policy has not been defined for the computer.
- *Applying policy*. Data encryption and / or decryption is in progress on the computer.
- Error! An error occurred during data encryption and / or decryption on the computer.

- *Reboot required*. The operating system has to be rebooted in order to start or finish data encryption or decryption on the computer.
- *Compliant with policy*. Data encryption on the computer has been completed using the encryption settings specified in the Kaspersky Security Center policy applied to the computer.
- *Canceled by user*. The user has declined to confirm the file encryption operation on the removable drive.

Viewing the encryption status

► *To view the encryption status of computer data:*

1. Open the Administration Console of Kaspersky Security Center.
2. 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.
3. In the workspace, select the **Devices** tab.

   The **Devices** tab in the workspace shows the properties of computers in the selected administration group.
4. On the **Devices** tab in the workspace, slide the scroll bar all the way to the right.
5. If the **Encryption status** column is not displayed:
   1. Right-click to open the context menu for the table header.
   2. In the context menu, in the **View** drop-down list, select **Add/Remove columns**.

      The **Add/Remove columns** window opens.
   3. In the **Add/Remove columns** window, select the **Encryption status** check box.
   4. Click **OK**.

   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, and about full disk encryption.

Viewing encryption statistics in details panes of Kaspersky Security Center

► *To view the encryption status in details panes of Kaspersky Security Center:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, select the **Administration Server – <Computer name>** node.
3. In the workspace to the right of the Administration Console tree, select the **Statistics** tab.
4. Create a new page with details panes containing data encryption statistics. To do so:
   a. On the **Statistics** tab, click the **Customize view** button.

      The **Properties: Statistics** window opens.

   b. In the **Properties: Statistics** window, click **Add**.

      The **Properties: New page** window opens.

   c. In the **General** section of the **Properties: New page** window, type the page name.

   d. In the **Details panes** section, click the **Add** button.

The **New details pane** window opens.

e. In the **New details panel** window in the **Protection status** group, select the **Encryption of devices** item.

f. Click **OK**.

The **Properties: Encryption Control** window opens.

g. If necessary, edit the details pane settings. To do so, use the **View** and **Devices** sections of the **Properties: Encryption of devices** window.

h. Click **OK**.

i. Repeat steps d – h of the instructions, selecting the **Encryption of removable drives** item in the **Protection status** section of the **New details pane** window.

The details panes added appear in the **Details panes** list in the **Properties: New page** window.

j. In the **Properties: New page** window, click **OK**.

The name of the page with details panes created at the previous steps appears in the **Pages** list of the **Properties: Statistics** window.

k. In the **Properties: Statistics** window, click **Close**.

5. On the **Statistics** tab, open the page that was created during the previous steps of the instructions.

The details panes appear, showing the encryption status of computers and removable drives.

Viewing file encryption errors on local computer drives

► *To view the file encryption errors on local computer drives:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Managed devices** folder of the Administration Console tree, open the folder with the name of the administration group that includes the client computer whose list of file encryption errors you want to view.
3. In the workspace, select the **Devices** tab.
4. On the **Devices** tab, select the name of the computer in the list and right-click to open the context menu.
5. Do one of the following:
   - In the context menu of the computer, select **Protection**.
   - In the context menu of the computer, select the **Properties** item. In the **Properties: <computer name>** window, select the **Protection** section.
6. In the **Protection** section of the **Properties: <computer name>** window, click the **View list of data encryption errors** link to open the **Data encryption errors** window.

   This window shows the details of file encryption errors on local computer drives. When an error is corrected, Kaspersky Security Center removes the error details from the **Data encryption errors** window.

Viewing the data encryption report

► *To view the data encryption report:*

1. Open the Administration Console of Kaspersky Security Center.

2. In the **Administration Server** node of the Administration Console tree, select the **Reports** tab.
3. Click the **Create report template** button.

   The Report Template Wizard starts.
4. Follow the instructions of the Report Template Wizard. In the **Select report template type** window in the **Other** section, select one of the following items:
   - **Managed device encryption status report**.
   - **Mass storage device encryption status report**.
   - **File encryption errors report**.
   - **Report on blocked access to encrypted files**.

   After you have finished with the New Report Template Wizard, the new report template appears in the table on the **Reports** tab.
5. Select the report template that was created at the previous steps of the instructions.
6. In the context menu of the template, select **Show report**.

The report generation process starts. The report is displayed in a new window.

Local tasks

This section contains information about the specifics of tasks and their configuration via Kaspersky Security Center.

In this section:

Task management section

The **Task management** section lets you configure management of local and group tasks from the Kaspersky Endpoint Security interface.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Allow use of local tasks

This check box allows / blocks operations with local tasks of Kaspersky Endpoint Security.

If the check box is selected, local tasks are displayed in the Kaspersky Endpoint Security local interface. When there are no additional policy restrictions, the user can configure and run tasks.

If the check box is cleared, use of local tasks is stopped. In this mode, local tasks do not run according to schedule. Tasks cannot be started or configured in the local interface of Kaspersky Endpoint Security, or when working with the command line.

You can still start a virus scan of a file or folder by selecting the **Scan for viruses** option in the context menu of the file or folder. The scan task is started with the default values of settings for the custom scan task.

This check box is cleared by default.

Allow group tasks to be displayed

This check box allows / blocks the display of group tasks that were created in Kaspersky Security Center from the Kaspersky Endpoint Security local interface.

If the check box is selected, the group tasks that were created in Kaspersky Security Center are displayed in the Kaspersky Endpoint Security local interface.

This check box is selected by default.

Allow management of group tasks

This check box allows / blocks the management of group tasks that were created in Kaspersky Security Center from the Kaspersky Endpoint Security local interface.

If the check box is selected, the management of group tasks that were created in Kaspersky Security Center from the Kaspersky Endpoint Security local interface, is allowed.

This check box is cleared by default.

Scan from context menu 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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the

Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.

- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

High

If the probability of computer infection is very high, select this file security level.

If this option is selected, Kaspersky Endpoint Security uses the deep level of heuristic analysis.

Recommended

This file security level is recommended for use by Kaspersky Lab specialists.

If this option is selected, Kaspersky Endpoint Security uses the medium level of heuristic analysis.

The **Recommended** file security level is selected by default.

Low

The settings of this file security level ensure maximum scanning speed.

If this option is selected, Kaspersky Endpoint Security uses the light level of heuristic analysis.

Custom

A file security level with your personal custom settings.

Settings

This button opens the Scan from context menu 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 Scan from context menu task detects infected files.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.

- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Disinfect, delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

This action is selected by default.

Disinfect, inform if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats.

Inform

If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.

Removable drives scan section

The **Scan removable drives on connection** section lets you configure a virus scan to be performed when a removable drive is connected to the computer.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Action on connection of a removable drive

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 email message

nws – new Microsoft Outlook Express email message

msg – Microsoft Mail email message

plg – email message

mbx – saved Microsoft Office Outlook email message

doc* – Microsoft Office Word documents, such as: doc for Microsoft Office Word documents, docx for Microsoft Office Word 2007 documents with XML support, and docm for Microsoft Office Word 2007 documents with macro support

dot* – Microsoft Office Word document templates, such as: dot for Microsoft Office Word document templates, dotx for Microsoft Office Word 2007 document templates, dotm for Microsoft Office Word 2007 document templates with macro support

fpm – database program, Microsoft Visual FoxPro start file

rtf – Rich Text Format document

shs – Windows Shell Scrap Object Handler fragment

dwg – AutoCAD® drawing database

msi – Microsoft Windows Installer package

otm – VBA project for Microsoft Office Outlook

pdf – Adobe Acrobat document

swf – Shockwave® Flash package object

jpg, jpeg – compressed image graphics format

emf – Enhanced Metafile format file. 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

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 **Action on connection of a removable drive** drop-down list.

If this check box is selected, Kaspersky Endpoint Security performs the action that is selected in the **Action on connection of a removable drive** 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 **Action on connection of a removable drive** 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 **Action on connection of a removable drive** drop-down list.

This check box is cleared by default.

Show scan progress

This check box enables / disables display of the progress of removable drive scans in a separate window and in the **Tasks** window.

If the check box is selected, Kaspersky Endpoint Security displays the progress of removable drive scans in a separate window and in the **Tasks** window.

If the check box is cleared, Kaspersky Endpoint Security starts removable drive scans in the background.

This setting is available if the **Detailed Scan** or **Quick Scan** action is selected in the **Action on connection of a removable drive** drop-down list.

This check box is selected by default.

Background scan section

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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Scan when the computer is idling

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.

General Settings

This section contains information about configuring the general settings of Kaspersky Endpoint Security.

In this section:

Application Settings section

The **Operating Mode** section lets you configure Kaspersky Endpoint Security to start when the computer is turned on, and enable or disable Advanced Disinfection technology.

Buttons 🔒 **and** 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Start Kaspersky Endpoint Security 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.

Enable Advanced Disinfection technology

> This check box is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. The check box 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 5).

This check box enables / disables the option whereby Kaspersky Endpoint Security uses advanced disinfection technology.

If the check box is selected, a pop-up notification is displayed on the screen when malicious activity is detected in the operating system. In its notification, Kaspersky Endpoint Security offers the user to perform Advanced Disinfection of the computer. After the user approves this procedure, Kaspersky Endpoint Security neutralizes the threat. 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, on detecting malicious activity in the operating system Kaspersky Endpoint Security carries out the disinfection procedure according to the current settings. No computer restart is performed after Kaspersky Endpoint Security neutralizes the threat.

This check box is selected by default.

Use Kaspersky Security Center as proxy server for activation

This check box enables / disables the use of Kaspersky Security Center as a proxy server when activating the application.

If the check box is selected, Kaspersky Security Center is used as a proxy server when activating the application.

This check box is cleared by default.

The **Self-Defense** section lets you configure protection against external interference in the operation of the computer.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the

Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.

- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

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 services

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 **Performance** section lets you configure optimum energy and computer resource consumption in the operation of Kaspersky Endpoint Security.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The

values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Postpone scheduled tasks while running on battery power

Computer scan tasks and database update tasks tend to consume considerable resources and take a long time to finish.

This check box enables / disables energy conservation mode when a portable computer is running on battery power, which postpones scan and update tasks.

If the check box is selected, energy conservation mode is enabled. Kaspersky Endpoint Security postpones scheduled tasks. The user can start scan and update tasks manually, if necessary.

If the check box is cleared, energy conservation mode is disabled. Scan and update tasks are started according to their respective schedules.

This check box is selected by default.

Concede resources to other applications

When Kaspersky Endpoint Security runs scheduled tasks, this may result in increased workload on the CPU and disk subsystems, which slows down the performance of other applications.

When the check box is selected, Kaspersky Endpoint Security suspends scheduled tasks when it detects an increased load and frees up operating system resources for user applications. This helps to relieve the load on the CPU and disk subsystems.

When the check box is cleared, scheduled tasks are performed without regard for the operation of other applications.

This check box is selected by default.

The **Proxy Server** section allows you to configure the connection to a proxy server used to connect to the Internet.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The

values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

Clicking the button opens the **Proxy server settings** window. This window lets you configure the proxy server used for Internet access.

The **Debug Information** section allows you to configure settings for working with dump and trace files.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

Clicking this button opens the **Debug information** window. In this window, you can configure the settings for working with dump files and trace files.

The **Computer status when settings are applied** section lets you configure the Administration Console to display the statuses of client computers with Kaspersky Endpoint Security installed.

In case of error when applying policy

The items in this drop-down list determine which computer status is displayed if an error occurred when policy settings were applied.

You can select the following list items:

- OK
- **Warning**.
- **Critical**.

The **Critical** item is selected by default.

In case of error when applying task

The items in this drop-down list determine which computer status is displayed if an error occurred when task settings were applied.

You can select the following list items:

- OK
- **Warning**.
- **Critical**.

The **Critical** item is selected 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 address

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.

Debug information window

Enable dump writing

Writing of dump files that can be used to examine Kaspersky Endpoint Security crashes.

If the check box is selected, Kaspersky Endpoint Security writes dumps when it crashes.

If the check box is cleared, Kaspersky Endpoint Security does not write dumps. The application also deletes existing dump files from the computer hard drive.

This check box is selected by default.

Enable dump and trace files protection

This check box enables / disables protection of dump files and trace files.

If the check box is selected, access to dump files is granted to the system and local administrators as well as to the user who enabled dump or trace file writing. Only system and local administrators can access trace files.

If the check box is cleared, any user can access dump files and trace files.

This check box is selected by default.

Exclusions section

The **Objects for detection** section lets you select the types of objects that Kaspersky Endpoint Security should monitor while it is running.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

This button opens the **Objects for detection** window. In this window, you can modify the list of objects 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 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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

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 exclusions 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 a list of exclusions 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 the File Threat Protection, Web Threat Protection, and Mail Threat Protection components scan incoming and outgoing data streams.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the

Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.

- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

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 only selected ports

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 and 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.

Trojan

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 **Packers** 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
- Selected files
- Folders
- Files and folders that are selected by a mask

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

- 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.
- **Object hash**. This column shows the SHA256 hash 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 malware detects an object with the specified hash.
- **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 **Scan exclusion** window. You can create a new exclusion in this window.

Edit

Clicking this button opens the **Scan exclusion** window. You can edit the settings of the selected exclusion in this window.

This button is available when an item is selected in the **Scan exclusions** 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 exclusions 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.

Object hash

This check box enables / disables the option that excludes a file with the specified hash from the virus scan.

Comment

A field for entering additional information about the exclusion.

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 during scans. You can also define a file or folder name mask.

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.

The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

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.

Object hash: enter the object hash

Clicking this link opens the **Object hash** window. In this window, you can define the SHA256 hash of an object to exclude from scanning.

Protection components: any / specified: select components

The **any** option signifies that this exclusion is used by all components of Kaspersky Endpoint Security.

The **specified** option 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** option is available if the **specified** option is available.

The **any** option 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.

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.

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:

Name of file or folder

Field for entering the file or folder name, or the mask of the file or folder name.

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

> Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
> The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

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

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\test** – Only the file C:\dir\test.

Browse

This button opens the **Select folder** window. You can select a file or folder in this window.

Include subfolders

This check box enables / disables an option whereby a folder is added to the exclusion 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.

Scan exclusions tab

Scan exclusions

This table contains information about scan exclusions.

You can exclude the following objects from scanning:

- Files of certain formats
- Selected files
- Folders
- Files and folders that are selected by a mask

A mask of a file or folder name is a representation of the name of a folder or name and extension of a file using common characters.

You can use the following characters to form a file or folder name mask:

- The * (asterisk) character, which takes the place of any set of characters in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**.txt will include all paths to files with the TXT extension located in folders on the C: drive, but not in subfolders.

> Two consecutive * characters take the place of any set of characters (including an empty set) in the file or folder name, including the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\***.txt will include all paths to files with the TXT extension located in any folder on the C: drive.
> The name and the extension of a file are always separated with a dot.

- The ? (question mark) character, which takes the place of any single character in the file or folder name, except the \ and / characters (delimiters of the names of files and folders in paths to files and folders). For example, the mask C:\**\???.txt will include paths to all files that have a name consisting of three characters and the TXT extension in folders on drive C:.
- All other characters permissible in the names of files and folders.

Kaspersky Endpoint Security blocks the input of the following characters that are invalid in file and folder names: <, >, |, ".

- 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.
- **Object hash**. This column shows the SHA256 hash 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 malware detects an object with the specified hash.
- **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 **Scan exclusion** window. You can create a new exclusion in this window.

Edit

Clicking this button opens the **Scan exclusion** window. You can edit the settings of the selected exclusion in this window.

This button is available when an item is selected in the **Scan exclusions** 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.

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 Application Control component regulates the startup of each of the applications regardless of whether or not the application is included in the table of trusted applications.

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 or disables the scan exclusion for all files opened by the specific application.

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 or disables monitoring of the file- and network activity of an application in the operating system by the Host Intrusion Prevention, Behavior Detection, Exploit Prevention, Remediation Engine 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 or disables the scan exclusion for network traffic generated by the specific application.

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 scan exclusion settings for network traffic.

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 Host Intrusion Prevention 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 Host Intrusion Prevention 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 **Select file or folder** window. 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 for Windows Administration Plug-in to generate a list of applications whose network activity should be monitored by Firewall via the 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.

Reports and Storage section

The **Reports** section lets you configure the application report storage settings.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Store reports no longer than

This check box enables / disables the option that defines the maximum report storage term. The maximum report storage term is measured in days.

When the check box is selected, the maximum storage term is limited by the amount of time that is specified in the field on the right. The default maximum storage term for reports is 30 days. After that period of time, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file.

This check box is selected by default.

Maximum file size

The check box enables / disables the option that defines the maximum report file size. The maximum report file size is specified in megabytes.

When the check box is selected, the maximum report file size is limited by the value that is specified in the field on the right. By default, the maximum file size is 1024 MB. To avoid exceeding the maximum report file size, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file when the maximum report file size is reached.

This check box is selected by default.

The **Backup** section lets you configure Backup settings.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Store objects no longer than

This check box enables / disables the option that defines the maximum storage period for copies of files in Backup. The maximum file storage term is measured in days.

When the check box is selected, the maximum storage term for files is limited by the amount of time that is specified in the field on the right. The default maximum storage term for files is 30 days. After expiration of the maximum storage term, Kaspersky Endpoint Security deletes the oldest files from Backup.

This check box is selected by default.

Maximum storage size

The check box enables / disables the option that defines the maximum data storage size. The data storage comprises storage for backup copies of files. The maximum size of the data storage is specified in megabytes.

When the check box is selected, the maximum storage size is limited by the value that is specified in the field on the right. By default, the maximum size is 100 MB. To not exceed the maximum data storage size, Kaspersky Endpoint Security automatically deletes the oldest files when the data storage reaches its maximum size.

This check box is cleared by default.

The **Data transfer to Administration Server** section lets you select which events on client computers must have their information relayed to the Administration Server.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

Clicking this button opens the **Inform** window.

Inform window

About files in Backup

This check box enables or disables the transmission of data on files placed in Backup to the Administration Server.

If the check box is selected, Kaspersky Endpoint Security sends events containing information about files placed in Backup to the Administration Server.

This check box is selected by default.

About unprocessed files

This check box enables / disables the transmission of data about active threats to the Administration Server.

If the check box is selected, Kaspersky Endpoint Security sends events containing information about active threats to the Administration Server.

This check box is selected by default.

About installed devices

This check box enables or disables the transmission of data on installed devices to the Administration Server.

If the check box is selected, Kaspersky Endpoint Security sends data on devices connected to the Kaspersky Endpoint Security client computer to the Server.

This check box is selected by default.

About started applications

This check box enables or disables the transmission of data on started applications to the Administration Server.

If the check box is selected, Kaspersky Endpoint Security sends data on executable files started on the Kaspersky Endpoint Security client computer to the Server.

This check box is selected by default.

About file encryption errors

This check box enables or disables the transmission of data on encryption component errors to the Administration Server.

If the check box is selected, Kaspersky Endpoint Security sends data about errors occurring during operation of encryption components to the Administration Server.

This check box 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.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Display 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.

Simplified application interface

The check box enables or disables the display of the main window of Kaspersky Endpoint Security.

If the check box is selected, the main application window is not available on the client computer that has Kaspersky Endpoint Security installed. Right-click to open the context menu for the Kaspersky Endpoint Security icon containing the following items:

- **Disable policy**. Disables the Kaspersky Security Center policy. This context menu item is available if a policy has been applied to the computer and a password for disabling the Kaspersky Security Center policy has been set.
- Tasks Drop-down list containing the following items:
  - **Integrity Check**.
  - Rollback
  - **Full Scan**.
  - **Custom Scan**.
  - **Critical Areas Scan**.
  - Updater
- **Support**. This opens the **Support** window containing information necessary for contacting Kaspersky Lab Technical Support.
- **Exit**. Version of Kaspersky Endpoint Security.

If the check box is cleared, the main application window is available on the client computer that has Kaspersky Endpoint Security installed.

This check box is available if the **Display application interface** check box is selected.

This check box is cleared by default.

The **Notifications** section lets you configure the settings of notifications about events that occur during the operation of Kaspersky Endpoint Security.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

Clicking this button opens the **Notifications** window. In this window you can configure notifications about events that occur during the operation of Kaspersky Endpoint Security and the logging of events in the local log of Kaspersky Endpoint Security and / or the Windows Event Log. The following notification types are available:

- Messages that are displayed above the application icon in the Microsoft Windows taskbar:
  - If you need to select a further action in connection with this event, Kaspersky Endpoint Security displays a notification window.
  - If no selection of a further action in connection with this event is needed, Kaspersky Endpoint Security shows a pop-up notification about the event.
- Email notifications.

The **Warnings** lets you specify which categories of application events should determine the appearance of the Kaspersky Endpoint Security icon in the taskbar notification area.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

Clicking this button opens the **Warnings** window. In this window, you can select the categories of application events that will determine the appearance of the Kaspersky Endpoint Security icon in the notification area.

The **Local anti-virus database status notifications** section lets you configure notifications about outdated anti-virus databases used by the application.

Buttons 🔒 **and** 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Send the "Databases out of date" notification if databases were not updated for N days

The application displays the "Databases are out of date" pop-up notification when the specified amount of time elapses after the previous database update.

The default value is three days.

Send the "Databases extremely out of date" notification if databases were not updated for N days

The application displays the "Databases are extremely out of date" pop-up notification when the specified amount of time elapses after the previous database update.

The default value is seven days.

The **Password protection** section lets you configure the password scope and enable a temporary password.

Buttons 🔒 **and** 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The

values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

This button opens the **Password protection** window. This window lets you configure the password scope.

The **User support** section lets you create a list of links to web resources containing information about technical support for Kaspersky Endpoint Security.

Buttons 🔒 and 🔓

The button with the closed "lock" means the following:

- Kaspersky Security Center blocks changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On all client computers, Kaspersky Endpoint Security uses the same values of these settings, i.e. the values that are defined in the policy properties.
- Kaspersky Security Center blocks changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings that are defined in top level policy properties are used.

The button with the open "lock" means the following:

- Kaspersky Security Center allows changes to settings in this settings group from the Kaspersky Endpoint Security interface on client computers. On each client computer, Kaspersky Endpoint Security operates according to the local values of these settings if the component is enabled.
- Kaspersky Security Center allows changes to settings in this settings group in the properties of those policies for nested administration groups and slave Administration Servers in which the **Inherit settings of top level policy** function is enabled. The values of these settings do not depend on what is specified in the top level policy properties.

The "lock" is closed by default.

Settings

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.

Notifications window

List of components and tasks

This list lets you select an application component or task for which you want to receive notifications and logging.

Kaspersky Endpoint Security components and tasks are grouped into the following four categories:

- **Advanced Threat Protection**. This category includes components that monitor application activity on the computer and provide this information to other components to ensure more effective protection of the computer.
- **Essential Threat Protection**. This category comprises components that protect the computer in real time across all routes of incoming and outgoing data.
- **Security Controls**. This category includes components that control the applications installed on the computer and access to connected devices and websites.
- **Endpoint Sensor**. This category includes the only Endpoint Sensor component that is intended for timely detection of threats such as targeted attacks. The component continually monitors processes, active network connections, and files that are modified, and relays this information to the Kaspersky Anti Targeted Attack Platform server.
- Tasks This category includes tasks that are used to keep application modules and databases up to date, scan files for viruses and other threats, and check the integrity of the application.
- **Data Encryption**. This category includes a single item: **Data encryption**. It corresponds to the components that support the encryption of hard drives and removable drives as well as file and folders on local drives of the computer.

The **Data Encryption** category is available if encryption components are installed on the computer.

The **System Audit** item is displayed first in the list of components and tasks. System Audit does not belong to any category. Events associated with this item occur during operation of the application in general as well as during user interaction with the application.

The list of Kaspersky Endpoint Security components and tasks is located in the left part of the window.

When you select a component or task in the list of components or tasks, the table in the right part of the window lists notification settings for the different importance levels of events that may occur during the operation of the selected component or while the selected task is running.

By default / Manually / Critical / Important / Informational

Items in this drop-down list allow automatically selecting the events about which you want to be notified or which you want to be logged.

The following items are available from the drop-down list:

- **By default**. If this item is selected, Kaspersky Endpoint Security logs information or sends event notifications according to settings recommended by Kaspersky Lab specialists.
- **Manually**. This item appears in the drop-down list as the selected item after any change has been made to the table by selecting or clearing a check box.

  This item is not displayed in the drop-down list until the first change made to the table manually and after selection of any other item in the list.
- **Critical**. If this item is selected, Kaspersky Endpoint Security logs information about

events that have the *Critical events* severity level (including *Functional failure* events for the **System audit** item and the **Application Control** component).

- **Important**. If this item is selected, Kaspersky Endpoint Security logs information about events that have the *Critical events* (including *Functional failure* events for the **System audit** feature and the **Application Control** component) and *Important events* severity levels.
- **Informational**. If this item is selected, Kaspersky Endpoint Security logs information about all events occurring during operation of the application.

Event notification settings

A table with the settings of notifications about events of different importance levels that may occur during the operation of a component, task, or the entire application. Kaspersky Endpoint Security shows notifications about these events on the screen, sends them by email, or logs them.

Events in the table are grouped by importance level. Events with the importance level of *Critical events* are shown at the top of the table, followed by *Important events*, with *Informational events* appearing at the bottom of the table. The *Functional failures* group is also available for the **System audit** item and the **Application Control** component. Such events belong to critical events in terms of their level of importance.

The table contains the following columns:

- **Event**. This column displays the icon that signifies the level of event importance and the text of the notification about this event.

  The following importance levels of events exist:

  - **Critical events** (⚠ icon). Events of high importance and faults that indicate problems in the operation of Kaspersky Endpoint Security or vulnerabilities in protection of the user's computer.
  - **Important events** (⚠ icon). Events that need attention because they reflect important situations in the operation of Kaspersky Endpoint Security.
  - **Informational events** (ℹ icon). Formal events that do not normally contain important information.
- **Save in local log**. This column shows the check box enables / disables the logging of the event notification in the Kaspersky Endpoint Security log.
- **Save in Windows Event Log**. This column shows the check box enables / disables the logging of the event notification in the Microsoft Windows event log.
- **Notify on screen**. This column shows a check box that enables / disables the display of event information on the screen. The pop-up notification is shown above the application icon in the Windows taskbar notification area.
- **Notify by email**. This column shows a check box that enables / disables the transmission of an event notification by email.

  This notification method requires configuring email notification delivery settings. To do so, click the **Email notification settings** button.

By default, the check boxes are selected according to the recommended notification settings of Kaspersky Endpoint Security.

Email notification settings

Clicking this button opens the **Email notification settings** window. This window lets you configure email notification settings.

Email notification settings window

Send event notifications

This check box enables / disables the option that sends email notifications about events in the operation of Kaspersky Endpoint Security.

When the check box is selected, Kaspersky Endpoint Security sends email notifications about events.

This check box is cleared by default.

The **Sending notifications on behalf of** section lets you specify the email address from which Kaspersky Endpoint Security sends notifications.

This section is available when the **Send event notifications** check box is selected.

Sender's address

Field for entering the email address from which Kaspersky Endpoint Security sends notifications.

SMTP server

Field for entering the address of the mail SMTP server through which Kaspersky Endpoint Security sends notifications.

For example, `mail.company.com`.

Port

Field for editing the number of the network port that Kaspersky Endpoint Security uses to send notifications.

The default value is 25.

User name

Field for entering the name of the user who owns the account on the SMTP server.

Password.

Field for entering the password of the user who owns the account on the SMTP server.

The **Notification recipient** field lets you specify the email address to which Kaspersky Endpoint Security sends notifications.

Recipient's address

Field for entering the email address to which Kaspersky Endpoint Security sends notifications.

Send test message

This button causes Kaspersky Endpoint Security to send a test message to the specified email address.

This button is available when the address of the SMTP mail server is specified in the **SMTP server** field and the **User name** field is not empty.

The **Send mode** section allows you to select the mode of sending notifications by email.

If event occurs

When this setting is selected, Kaspersky Endpoint Security sends an email message as soon as an event occurs.

This setting is selected by default.

By schedule

When this setting is selected, Kaspersky Endpoint Security sends an email message with event notices according to the specified schedule.

Edit

Clicking this button opens the **Schedule for sending email notifications** window. This window lets you create a schedule according to which Kaspersky Endpoint Security sends event notifications by email.

This button is available if the **By schedule** setting is selected.

Schedule for sending email notifications window

Frequency

A drop-down list whose items define the time interval between the email notifications that Kaspersky Endpoint Security sends.

The following items are available from the drop-down list:

- **Minutes**. When this item is selected, the time interval between email notifications is measured in minutes.
- **Hours**. When this item is selected, the time interval between email notifications is measured in hours.
- **Days**. When this item is selected, the time interval between email notifications is measured in days.
- **Every week**. When this item is selected, Kaspersky Endpoint Security sends notifications on the specified days of the week.
- **At a specified time**. When this item is selected, Kaspersky Endpoint Security sends notifications on the specified day and at the specified time.
- **Every month**. When this item is selected, Kaspersky Endpoint Security sends notifications once per month on the specified day and at the specified time.
- **After application startup**. When this item is selected, Kaspersky Endpoint Security sends notifications after each startup.

Run every

A field for entering a time interval at which Kaspersky Endpoint Security resends notifications.

This field is available if the following items are selected in the **Frequency** drop-down list: **Minutes**, **Hours**, **Days**, or **Every month**:

- If the item selected in the **Frequency** drop-down list is **Minutes**, you can specify a time interval in minutes in the **Run every** field. The value cannot exceed 59 minutes. The default value is 5 minutes.
- If the item selected in the **Frequency** list is **Hours**, you can specify a time interval in hours in the **Run every** field. The value cannot exceed 23 hours. The default value is one hour.
- If the item selected in the **Frequency** drop-down list is **Days**, you can specify a time interval in days in the **Run every** field. The value cannot exceed 31 days. The default value is one day.
- If the item selected in the **Frequency** list is **Every month**, in the **Run every** field you can type the day of the month on which Kaspersky Endpoint Security sends event notifications by email. The value cannot be later than the 31st day of the month. The first day of the month is the default value.

Start time

A field for entering the time of day when Kaspersky Endpoint Security sends event notifications by email.

This field is available if the following items are selected in the **Frequency** drop-down list: **Every week**, **Every month**, or **Days**.

The time is specified in HH:MM format. By default, it is set to 00:00.

Start on

The check boxes enable / disable the sending of notifications on the selected days of the week.

If the check box that corresponds to a day of the week is selected, on this day Kaspersky Endpoint Security sends notifications by email at the time that is specified in the **Start time** field.

The check boxes are available when the item selected in the **Frequency** drop-down list is **Every week**.

The check boxes that correspond to all days of the week are cleared by default.

Start date and time

A field for entering the date and time when Kaspersky Endpoint Security sends notifications by email.

This field is available when the item selected in the **Frequency** drop-down list is **At a specified time**.

The date is specified in DD / MM / YY format; the time is set in HH:MM:SS format. By default the field contains the current date, and the time is set to 0:00:00.

Postpone running after application startup for / **Start in**

A field for entering a time interval, measured in minutes, after startup of Kaspersky Endpoint Security. After this time, Kaspersky Endpoint Security sends notifications by email.

The default value is 0 minutes.

The **Postpone running after application startup for** field is available when any item except **After application startup** is selected in the **Frequency** drop-down list.

The **Start in** field is available when the item selected in the **Frequency** drop-down list is **After application startup**.

Warnings window

Active threats

The check box enables / disables the display of messages about the presence of active threats.

If the check box is selected and active threats are present, the Kaspersky Endpoint Security icon in the notification area of the Microsoft Windows task bar changes and a pop-up notification appears.

This check box is selected by default.

Computer restart required

The check box enables / disables the display of messages in the notification area about the need to restart the computer.

If the check box is selected and the computer needs to be restarted, the Kaspersky

Endpoint Security icon in the notification area of the Microsoft Windows task bar changes and a pop-up notification appears.

This check box is selected by default.

Problems with antivirus databases

The check box enables / disables the display of messages in the notification area about problems with the antivirus databases.

If the check box is selected and there are problems with the antivirus databases, the Kaspersky Endpoint Security icon in the notification area of the Microsoft Windows task bar changes and a pop-up notification appears.

This check box is selected by default.

Problems with protection level

The check box enables / disables the display of messages in the notification area about problems with the protection level.

If the check box is selected and there are problems with the protection level, the Kaspersky Endpoint Security icon in the notification area of the Microsoft Windows task bar changes and a pop-up notification appears.

This check box is selected by default.

Problems with license

The check box enables / disables the display of messages in the notification area about problems with the license.

If the check box is selected and there are problems with the license, the Kaspersky Endpoint Security icon in the notification area of the Microsoft Windows task bar changes and a pop-up notification appears.

This check box is selected by default.

Updates available

The check box enables / disables the display of messages in the notification area about available updates.

If the check box is selected and updates are available, the Kaspersky Endpoint Security icon in the notification area of the Microsoft Windows task bar changes and a pop-up notification appears.

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.

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.

Confirm password

Password confirmation field. It is required to rule out the possibility of a mistake in password entry.

The **Password scope** section lets you specify which operations cannot be performed until the defined password is entered.

Configure application settings

The check box enables / disables requests for the user name and 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 the user name and password before saving changes to settings.

Exit 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:

- Behavior Detection.
- Exploit Prevention.
- Host Intrusion Prevention.
- File Threat Protection.
- Web Threat Protection.
- Mail Threat Protection.
- Network Threat Protection.
- BadUSB Attack Prevention.

This check box is cleared by default.

Disable 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 Control.
- Device Control.
- Web Control.

This check box is cleared by default.

Disabling the Kaspersky Security Center policy

This check box enables / disables the user name and password prompt when the user attempts to disable the Kaspersky Security Center policy.

If the check box is selected and the user attempts to disable the Kaspersky Security Center policy, Kaspersky Endpoint Security prompts the user to enter the user name and password.

If the check box is cleared, the **Disable policy** item in the context menu of the Kaspersky Endpoint Security application icon is not available for selection.

This check box is cleared by default.

Remove key

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 the 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 the password.

This check box is cleared by default.

Restore 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 the password.

This check box is cleared by default.

View 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.

Restoring from Backup

This check box enables / disables the password prompt on the user's attempt to restore files from Backup.

If the check box is selected and the user attempts to restore files from Backup, Kaspersky Endpoint Security prompts the user to enter the password.

This check box is selected by default.

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.

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.

Link to web resource window

Name

Field for entering the name of a web resource.

Address

Field for entering the address of a web resource.

Description

Field for entering the description of a web resource.

Task management

This section describes how to manage tasks for Kaspersky Endpoint Security. For more details on task management through Kaspersky Security Center, please refer to the Kaspersky Security Center Help Guide.

In this section:

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.

  > If the Application Control component is not installed on a computer with Kaspersky Endpoint Security installed, the inventory task on this computer will return an error.

- Updater 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 group 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

When the check box is selected, Kaspersky Endpoint Security applies the selected key file to add an additional key.

When the check box is cleared, Kaspersky Endpoint Security applies the selected key file to add the active key.

This check box is cleared by default.

Information about the key

This section shows the properties of the key that is added on the computer(s) as a result of the add key task:

- key;
- license type (commercial or trial);
- license validity period;
- license expiration date;
- application functionality available under the license.

List of keys in Kaspersky Security Center storage window

Key

This column shows a key.

License type

This column shows the license type: commercial or trial.

License term

This column shows the license validity period.

Expiration date

This column shows the key expiration date.

Protection

This column shows an icon. The icon signifies the status of availability of protection components:

- The ✗ icon signifies that protection components are unavailable.
- The ✓ icon signifies that protection components are available.

Security Controls

This column shows an icon. The icon signifies the status of availability of security components:

- The ✗ icon signifies that security components are unavailable.
- The ✓ icon signifies that security components are available.

Data Encryption

This column shows an icon. The icon signifies the status of availability of encryption functionality:

- The ✗ icon signifies that encryption functionality is unavailable.
- The ✓ icon signifies that encryption functionality is available.

List of activation codes in Kaspersky Security Center storage window

Key

This column shows a key.

License type

This column shows the license type: commercial or trial.

License term

This column shows the license validity period.

Expiration date

This column shows the key expiration date.

Protection

This column shows an icon. The icon signifies the status of availability of protection components:

- The ✗ icon signifies that protection components are unavailable.
- The ✓ icon signifies that protection components are available.

Security Controls

This column shows an icon. The icon signifies the status of availability of security components:

- The ✗ icon signifies that security components are unavailable.
- The ✓ icon signifies that security components are available.

Data Encryption

This column shows an icon. The icon signifies the status of availability of encryption functionality:

- The ✗ icon signifies that encryption functionality is unavailable.
- The ✓ icon signifies that encryption functionality is available.

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 drop-down list located in the upper-right part of the window contains the following items that determine the type of Kaspersky Endpoint Security installation on client computers:

- **Basic installation**. If this item is selected, only protection components are installed to the user's computer.
- **Standard installation**. If this item is selected, protection components and control components are installed on the user's computer. This item is selected by default.
- **Custom installation**. If this item is selected, you can select the components to be installed and specify the destination folder for the application. This type of installation lets you install the components that are not included in the basic and standard installations.

The contents of the installation package are determined by the check boxes opposite the names of Kaspersky Endpoint Security components grouped into the following five sections:

- **Advanced Threat Protection**.
- **Essential Threat Protection**.
- **Security Controls**.
- **Data Encryption**.
- **Endpoint Sensor**.

If the check box opposite a component name is selected, the installation package installs the component on the user's computer with the settings recommended by Kaspersky Lab experts.

When the check box opposite the component name is cleared, the component is not installed on the user's computer as part of the installation package.

The check box for the File Threat Protection component cannot be cleared.

The set of check boxes selected by default depends on the selected type of installation.

Remove incompatible third-party applications

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.

Advanced settings window

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.

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.

Inventory task settings section

The check box opposite an item in the **Inventory scope** list includes / excludes the corresponding folder from the inventory scope.

Add

Clicking this button opens the **Select scan scope** window. This window lets you select an object to add to the inventory scope.

When forming the inventory scope, you can use environment variables such as %SystemRoot%. These variables must be general system variables for correct execution of the inventory task on all computers that have Kaspersky Endpoint Security installed.

Edit

Clicking this button opens the **Select scan scope** window. This window lets you change the object included in the inventory scope.

Delete

Clicking this button causes Kaspersky Endpoint Security to delete the inventory object selected in the **Inventory scope** list from the inventory scope.

This button is available if an object is selected in the **Inventory scope** list.

To temporarily exclude an object from the inventory scope, clear the check box next to its name in the **Inventory scope** list.

Scan when the computer is idling

This check box enables / disables a function that suspends starting the inventory task when computer resources are limited. Kaspersky Endpoint Security pauses the inventory task if the screensaver is off and the computer is unlocked.

By default, the check box is not selected.

DLL modules inventory

This check box enables / disables the function that analyzes data on DLL modules and relays it to the Administration Server.

By default, the check box is not selected.

Script files inventory

This check box enables / disables the function that analyzes data on files containing scripts and relays the analysis results to the Administration Server.

Kaspersky Endpoint Security recognizes scripts in the following types of files:

- Package files (batch, ps1);
- JavaScript files (js);
- Visual Basic Script files (vbs);
- Windows registry files (reg);
- Metro app files;
- Java Archive executable packages (jar);
- PowerShell files (ps1).

By default, the check box is not selected.

Additional

This button opens the **Advanced Settings** window. This window lets you set the file scan settings during the inventory task.

List of activation codes in Kaspersky Security Center storage window

Key

This column shows a key.

License type

This column shows the license type: commercial or trial.

License term

This column shows the license validity period.

Expiration date

This column shows the key expiration date.

Protection

This column shows an icon. The icon signifies the status of availability of protection components:

- The ✗ icon signifies that protection components are unavailable.
- The ✓ icon signifies that protection components are available.

Security Controls

This column shows an icon. The icon signifies the status of availability of security components:

- The ✗ icon signifies that security components are unavailable.
- The ✓ icon signifies that security components are available.

Data Encryption

This column shows an icon. The icon signifies the status of availability of encryption functionality:

- ✗ The icon signifies that encryption functionality is unavailable.
- ✓ The icon signifies that encryption functionality is available.

Update group task settings section

In the **Update settings for local mode** section, you can configure the settings that are applied when running the update task if communication is established between Kaspersky Security Center and the computer on which the application has been installed.

In the **Update settings for mobile mode** section, you can configure the settings that are applied when running the update task if no connection is established between the computer on which the application is installed and Kaspersky Security Center (for example, if the computer is not connected to the Internet).

Settings

This button opens the **Source** tab in the **Update** window. The **Source** tab lets you specify paths to update sources and select the region where the nearest Kaspersky Lab update server is located.

Information about the current update source is displayed on the right of the button.

Download updates of application modules

This check box enables / disables downloads of application module updates along with anti-virus database updates.

If the check box is selected, Kaspersky Endpoint Security notifies the user about available application module updates and includes application module updates in the update package while running the update task. The way application module updates are applied is determined by the following settings:

- **Install critical and approved updates**. If this option is selected, when application module updates are available Kaspersky Endpoint Security installs critical updates automatically and all other application module updates only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center.
- **Install only approved updates**. If this option is selected, when application module updates are available Kaspersky Endpoint Security installs them only after their installation is approved locally via the application interface or on the side of Kaspersky Security Center. This option is selected by default.

If the check box is cleared, Kaspersky Endpoint Security does not notify the user about available application module updates and does not include application module updates in the update package while running the update task.

If application module updates require reviewing and accepting the terms of the End User License Agreement, the application installs updates after the terms of the End User License Agreement have been accepted.

This check box is selected by default.

Copy updates to folder

To save Internet traffic, you can configure Kaspersky Endpoint Security updates so that computers on your LAN receive updates from a shared folder. To do this, one of the computers on your LAN receives the up-to-date update package from Kaspersky Lab update servers and then copies the retrieved update package to a shared folder. After that, other computers on your LAN are able to receive the update package from this shared folder.

This check box enables / disables the copying of the update package to the shared folder. This reduces Internet traffic because the update package is downloaded only once.

If this check box is selected, Kaspersky Endpoint Security copies the update package to the folder C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\.

This check box is cleared by default.

Browse

This button opens the **Select folder** window. This window lets you select the target shared folder for the update package.

The path to the shared folder is shown to the left of the **Browse** button. You can also enter the path to the shared folder manually.

This field can be edited if the **Copy updates to folder** check box is selected.

Virus scan group task 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

This button opens the virus scan task settings window.

By default

This button sets the file security level to **Recommended**.

In the **Scan scope** section, you can select the objects to be scanned by Kaspersky Endpoint Security during a virus scan task.

Settings

Clicking this button opens the **Scan scope** window. This window lets you specify the objects to be scanned by the application during the virus scan task.

The **Run mode** section contains the settings that Kaspersky Endpoint Security uses to start the Custom Scan task.

Run only when the computer is idling

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 is performed by Kaspersky Endpoint Security after the virus scan detects infected files.

Disinfect, delete if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection fails, Kaspersky Endpoint Security deletes the files.

This action is selected by default.

Disinfect, inform if disinfection fails

If this option is selected, Kaspersky Endpoint Security automatically attempts to disinfect all infected files that are detected. If disinfection is not possible, Kaspersky Endpoint Security adds the information about the infected files that are detected to the list of active threats.

Inform

If this option is selected, Kaspersky Endpoint Security adds the information about infected files to the list of active threats on detection of these files.

Run Advanced Disinfection immediately

> Advanced Disinfection during a virus scan task on a computer is performed only if the Advanced Disinfection feature is enabled in the properties of the policy applied to this computer.

If the check box is selected, Kaspersky Endpoint Security performs Advanced Disinfection as soon as an active infection is detected during a virus scan task. After performing Advanced Disinfection, Kaspersky Endpoint Security restarts the computer without prompting the user for confirmation.

If the check box is cleared, Kaspersky Endpoint Security does not perform Advanced Disinfection as soon as an active infection is detected during a virus scan task. The application generates events involving detection of an active infection in local reports of the application and on the side of Kaspersky Security Center. Advanced Disinfection can be performed when the virus scan task is restarted with the **Run Advanced Disinfection immediately** check box selected. This enables the system administrator to choose a suitable time for running Advanced Disinfection on computers and then having them restarted automatically.

This check box is cleared by default.

Authentication Agent account management group 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.

Add user account window

Windows account

Field for entering the name of an operating system user account. An Authentication Agent account will be created based on this user account.

You can type the name of the user account manually or select it in the standard Microsoft Windows dialog **Select users or groups**. The Microsoft Windows dialog **Select users or groups** opens when you click the **Select** button.

A user account name is necessary to obtain an SID. An SID is a unique security ID that helps the system to differentiate between identically named user accounts.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window, you can select a Microsoft Windows user account. The name of the selected user account is displayed in the **Windows account** field.

After the **Select Users or Groups** dialog in Microsoft Windows is closed, the SID of the selected user account is determined automatically.

Allow

Clicking this button determines the security identifier (SID) of the user account. Kaspersky Endpoint Security scans all local and domain accounts accessible on the computer with the Administration Console installed. If the user account name matches the name specified in the **Windows account** field, Kaspersky Endpoint Security displays the SID of this account in the **SID** string.

If you manually specified the user account name but did not determine its SID using the **Resolve** button, the SID will be determined when the task is run. The search will be performed among local and domain accounts accessible on the computer on which the task is run.

User name

Field for entering the name of the Authentication Agent account. The Authentication Agent account name must be entered during the authentication procedure in order to access encrypted hard drives. The Authentication Agent account name may differ from the Microsoft Windows user account name.

The Authentication Agent account name must not include hieroglyphs or be longer than 256 characters.

By default, the field duplicates the Microsoft Windows account user name specified in the **Windows account** field.

Allow password-based authentication

This check box enables / disables the option for requiring an Authentication Agent account password to access encrypted hard drives (if the **Allow certificate-based authentication** check box is cleared and a token or smart card is not connected).

If the check box is selected, the application requires that the user enter an Authentication Agent account password to access encrypted hard drives.

This check box is selected by default.

Password.

Field for entering the password of the Authentication Agent account. The password is needed to pass authentication in order to access encrypted hard drives.

The Authentication Agent account password must consist of only ASCII characters and be no longer than 128 characters.

Confirm password

Password confirmation field. It is required to rule out the possibility of a mistake in password entry.

Password change upon authentication in Authentication Agent

Password change procedure upon first user authentication in the Authentication Agent:

- **Change password upon first authentication**. Kaspersky Endpoint Security prompts the user to change the password upon first authentication in the Authentication Agent under the account specified in the command. The new password cannot be viewed by the administrator in the properties of the Authentication Agent account.

  By default, this option is selected.
- **Do not require password change**. Kaspersky Endpoint Security does not prompt the user to change the password upon first authentication in the Authentication Agent under the account specified in the command.

Allow certificate-based authentication

This check box enables / disables the option to use a token or smart card to access encrypted hard drives.

If the check box is selected, the application requires the user to connect a token or smart card to the computer in order to access encrypted hard drives.

If the check box is cleared, the application does not allow user authentication even if a token or smart card is connected to the computer. If this is the case, only authentication with Authentication Agent account credentials is available.

This check box is cleared by default.

Browse

Clicking this button opens the standard **Select certificate file** window in Microsoft Windows. This window lets you specify the file of the token or smart-card digital certificate.

After the digital certificate file has been downloaded, the **Certificate Information** section shows fields with information about the certificate parameters.

Details

Clicking this link opens a window with the properties of the selected digital certificate.

This link is available if the digital certificate file is specified.

Command description

Field for entering any account information that you may need to manage the account.

Allow authentication

If this option is selected, the user working under the account specified in the command is allowed to complete authentication in the Authentication Agent.

By default, this option is selected.

Block authentication

If this option is selected, the user working under the account specified in the command is blocked from completing authentication in the Authentication Agent.

Edit user account window

Windows account

Field for entering the name of an operating system user account. An Authentication Agent account will be created based on this user account.

You can type the name of the user account manually or select it in the standard Microsoft Windows dialog **Select users or groups**. The Microsoft Windows dialog **Select users or groups** opens when you click the **Select** button.

A user account name is necessary to obtain an SID. An SID is a unique security ID that helps the system to differentiate between identically named user accounts.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window, you can select a Microsoft Windows user account. The name of the selected user account is displayed in the **Windows account** field.

After the **Select Users or Groups** dialog in Microsoft Windows is closed, the SID of the selected user account is determined automatically.

Allow

Clicking this button determines the security identifier (SID) of the user account. Kaspersky Endpoint Security scans all local and domain accounts accessible on the computer with the Administration Console installed. If the user account name matches the name specified in the **Windows account** field, Kaspersky Endpoint Security displays the SID of this account in the **SID** string.

If you manually specified the user account name but did not determine its SID using the **Resolve** button, the SID will be determined when the task is run. The search will be performed among local and domain accounts accessible on the computer on which the task is run.

Change user name

If the check box is selected and the task is run for all Authentication Agent accounts that were created based on the Microsoft Windows user account with the name specified in the **Windows account** field, Kaspersky Endpoint Security changes the user name to the name specified in the field below.

This check box is cleared by default.

User name

Field for entering the name of the Authentication Agent account. The Authentication Agent account name must be entered during the authentication procedure in order to access encrypted hard drives. The Authentication Agent account name may differ from the Microsoft Windows user account name.

The Authentication Agent account name must not include hieroglyphs or be longer than 256 characters.

By default, the field duplicates the Microsoft Windows account user name specified in the **Windows account** field.

Modify password-based authentication settings

If the check box is selected, password-based authentication settings can be edited.

This check box is cleared by default.

Allow password-based authentication

This check box enables / disables the option for requiring an Authentication Agent account password to access encrypted hard drives (if the **Allow certificate-based authentication** check box is cleared and a token or smart card is not connected).

If the check box is selected, the application requires that the user enter an Authentication Agent account password to access encrypted hard drives.

This check box is selected by default.

Password.

Field for entering the password of the Authentication Agent account. The password is needed to pass authentication in order to access encrypted hard drives.

The Authentication Agent account password must consist of only ASCII characters and be no longer than 128 characters.

Confirm password

Password confirmation field. It is required to rule out the possibility of a mistake in password entry.

Edit the rule of password change upon authentication in Authentication Agent

If the check box is selected and the task is run for all Authentication Agent accounts that were created based on the Microsoft Windows user account with the name indicated in the **Windows account** field, Kaspersky Endpoint Security changes the password change setting value to the value indicated in the field below.

This check box is cleared by default.

Password change upon authentication in Authentication Agent

Password change procedure upon first user authentication in the Authentication Agent:

- **Change password upon first authentication**. Kaspersky Endpoint Security prompts the user to change the password upon first authentication in the Authentication Agent under the account specified in the command. The new password cannot be viewed by the administrator in the properties of the Authentication Agent account.

  By default, this option is selected.
- **Do not require password change**. Kaspersky Endpoint Security does not prompt the user to change the password upon first authentication in the Authentication Agent under the account specified in the command.

Modify certificate-based authentication settings

If the check box is selected, certificate-based authentication settings can be edited.

This check box is cleared by default.

Allow certificate-based authentication

This check box enables / disables the option to use a token or smart card to access encrypted hard drives.

If the check box is selected, the application requires the user to connect a token or smart card to the computer in order to access encrypted hard drives.

If the check box is cleared, the application does not allow user authentication even if a token or smart card is connected to the computer. If this is the case, only authentication with Authentication Agent account credentials is available.

This check box is cleared by default.

Browse

Clicking this button opens the standard **Select certificate file** window in Microsoft Windows. This window lets you specify the file of the token or smart-card digital certificate.

After the digital certificate file has been downloaded, the **Certificate Information** section shows fields with information about the certificate parameters.

Details

Clicking this link opens a window with the properties of the selected digital certificate.

This link is available if the digital certificate file is specified.

Edit command description

If the check box is selected, when the task is performed for all Authentication Agent accounts created based on the Microsoft Windows user account with the name indicated in the **Windows account** field, Kaspersky Endpoint Security changes the command description to the description indicated in the field below.

This check box is cleared by default.

Edit the rule of access to authentication in Authentication Agent

If the check box is selected, when the task is performed for all Authentication Agent accounts created based on the Microsoft Windows user account with the name indicated in the **Windows account** field, Kaspersky Endpoint Security changes the rule of user access to the authentication dialog in the Authentication Agent to the rule indicated below.

This check box is cleared by default.

Allow authentication

If this option is selected, the user working under the account specified in the command is allowed to complete authentication in the Authentication Agent.

By default, this option is selected.

Block authentication

If this option is selected, the user working under the account specified in the command is blocked from completing authentication in the Authentication Agent.

Delete user account window

Windows account

Field for entering the name of an operating system user account. An Authentication Agent account will be created based on this user account.

You can type the name of the user account manually or select it in the standard Microsoft Windows dialog **Select users or groups**. The Microsoft Windows dialog **Select users or groups** opens when you click the **Select** button.

A user account name is necessary to obtain an SID. An SID is a unique security ID that helps the system to differentiate between identically named user accounts.

Select

This button opens the standard **Select Users or Groups** dialog in Microsoft Windows. In this window, you can select the user account to delete from the list of Authentication Agent accounts.

Allow

Clicking this button determines the SID of the user account whose name you manually entered in the **Windows account** field and that has been created in the operating system of the computer on which the Kaspersky Security Center Administration Server is installed.

If you manually specified the user account name but did not determine its SID by clicking the **Resolve** button, the SID will be determined when the task is performed on the computer.

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

The following commands are available for working with the application from the command line:

Таблица 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 Backup.
`EXPORT`	Export application settings.
`IMPORT`	Import application settings.
`ADDKEY`	Add a key.
`LICENSE`	Perform operations with a license.

Commands	Action
`PBATESTRESET`	Delete information about the compatibility of the system hard drive and Authentication Agent (for more detailed information, please refer to the *Administrator's Guide*).
`EXIT`	close the application
`EXITPOLICY /password=<password>`	Disable a Kaspersky Security Center policy (password-protected operation).
`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.
`PATCHCOMPATIBILITYRESET 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][/@:<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.
- `/@:<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.

To get the list of available profiles, run the following command:

```
avp.com help START
```

Examples:

```
avp.com START Scan_Objects
```

STOP command

Use:

```
STOP <Profile> /login=<login> /password=<password>
```

`<Profile>` parameter - profile name.

To get the list of available profiles, run the following command:

```
avp.com HELP STOP
```

STATUS command

Use:

```
STATUS [Profile]
```

To list all tasks, run STATUS command without parameters.

STATISTICS command

Use:

```
STATISTICS <Profile>
```

To list all tasks, run STATUS command without parameters.

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`

To get the list of available profiles, run the following command:

```
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:

Таблица 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 message in the command line	Shell return code
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: 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 license	_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 message in the command line	Shell return code
`Error: Configuration file not specified (/C)`	
`Error: Credential is not obtained, access denied`	
`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: 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 message in the command line	Shell return code
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	
Failed to get AVP_SERVICE_PRODUCT. Error	SHELL_RET_FAILED
Disable command cannot be elevated. Error	SHELL_RET_FAILED
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.

Таблица 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`

Character-based values	Numeric values	Available for commands
_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
_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_DETECTION	3	UPDATE ROLLBACK SCAN
[1-127]	[1-127]	LICENSE: /Check /Add (ActivateByCode) /Add (ActivateByKeyEx) /AddTicket
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 PATCHCOMPATIBILITYRESET SCAN
-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 PATCHCOMPATIBILITYRESET 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 PATCHCOMPATIBILITYRESET SCAN
-SHELL_RET_PARAMETER_INVALID	-1	LICENSE: /Add (ActivateByKeyEx) /AddTicket
SHELL_RET_SCAN_ALL_THREATED	101	UPDATE ROLLBACK SCAN
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

Character-based values	Numeric values	Available for commands
SHELL_RET_TASK_FAILED	3	STOP EXPORT IMPORT ADDKEY UPDATE ROLLBACK RESTORE SCAN
-SHELL_RET_TASK_FAILED	-3	LICENSE: /Add (ActivateByKey) /Add (ActivateByKeyEx) /AddTicket
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\KES\profiles` or `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\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

If you cannot find a solution to your problem in the application documentation or in one of the sources of information about the application, you are advised to contact Technical Support. Technical Support specialists will answer your questions about installing and using the application.

Before contacting Technical Support, please read the technical support rules (https://support.kaspersky.com/support/rules#en_us).

You can contact Technical Support in one of the following ways:

- By calling Technical Support (https://support.kaspersky.com/b2c).
- 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. For information on how to receive technical support in your region and Technical Support contact information, please visit the Kaspersky Lab Technical Support website (https://support.kaspersky.com/b2c).

> Before contacting Technical Support, please read the technical support rules (https://support.kaspersky.com/support/rules#en_us).

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.

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 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 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

► *To create a trace file:*

1. Open the main application window.
2. In the main application window, click the **Support** button.

   The **Support** window opens.
3. In the **Support** window, click the **System tracing** button.

   The **Information for Technical Support** window opens.
4. To start the trace process, select one of the following items in the **Traces** drop-down list:
   - **is enabled**

     Select this item to enable tracing.
   - **with rotation**.

     Select this item to enable tracing and limit the maximum number of trace files and the maximum size of each trace file. If the maximum number of trace files of the maximum size is written, the oldest trace file is deleted so that a new trace file can be written.

     If this item is selected, you can specify a value for the following fields:
     - **Maximum number of files for rotation**

       In this field, you can specify the maximum number of trace files written.
     - **Maximum size for each file**

       In this field, you can specify the maximum size of each trace file written.
5. 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)**.

6. Restart the computer.
7. To stop the trace process, return to the **Information for Technical Support** window and select **Disabled** in the **Traces** drop-down list.

After creating the trace file, you can proceed to uploading the trace results to the Kaspersky Lab server.

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 the computer as long as the application is in use, and are deleted permanently 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`.

The Authentication Agent trace file is stored in the System Volume Information folder and has the following name: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

You can view data saved in trace files.

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 Threat Protection 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.

Contents and storage of dump files

> The user is personally responsible for ensuring the safety of data collected, particularly for controlling and restricting access to collected data stored on the computer.

Dump files are stored on the computer as long as the application is in use, and are deleted permanently when the application is removed. Dump files are stored in the folder ProgramData\Kaspersky Lab.

A dump file contains all information about the working memory of Kaspersky Endpoint Security processes at the moment when the dump file was created. A dump file may also contain personal data.

Enabling and disabling dump writing

► *To enable or disable dump writing:*

1. Open the application settings window.
2. In the left part, select **Application Settings** in the **General Settings** section.

   The application settings are displayed in the right part of the window.
3. In the **Debug information** section, click the **Settings** button.

   The **Debug information** window opens.
4. Do one of the following:
   - Select the **Enable dump writing** check box if you want the application to write dumps of the application.
   - Clear the **Enable dump writing** check box if you do not want the application to write dumps of the application.
5. Click **OK** in the **Debug information** window.
6. To save the changes, click the **Save** button in the main application window.

Enabling and disabling protection of dump files and trace files

Dump files and trace files contain information about the operating system, and may also contain user data (see section "Contents and storage of trace files" on page 399). 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:*

1. Open the application settings window.
2. In the left part, select **Application Settings** in the **General Settings** section.

   The application settings are displayed in the right part of the window.
3. In the **Debug information** section, click the **Settings** button.

   The **Debug information** window opens.
4. 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.
5. Click **OK** in the **Debug information** window.

6. 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.