

Kaspersky Endpoint Security 8 for Windows®

KASPERSKY **lab**

Administrator Guide

APPLICATION VERSION: 8.0

Dear User,

Thank you for choosing our product! We hope that you will find this documentation useful and that it will provide answers to most questions that may arise.

Warning: This document is the property of Kaspersky Lab ZAO (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction or distribution of this document or parts hereof will result in civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, may be allowed only with written permission from Kaspersky Lab.

This document and related graphic images can be used exclusively for informational, non-commercial, or personal use.

This document may be amended without prior notice. The latest version of this document can be found on the Kaspersky Lab website, at <http://www.kaspersky.com/docs>.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm that may arise out of using such materials.

Document revision date: 9/30/11

© 2011 Kaspersky Lab ZAO. All Rights Reserved.

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

CONTENTS

ABOUT THIS GUIDE	10
In this Guide	10
Document conventions	11
SOURCES OF INFORMATION ABOUT THE APPLICATION	13
Sources of information for independent research	13
Discussing Kaspersky Lab applications on the Forum	14
Contacting the Documentation Development Team by email	14
KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS	15
What's new	15
Distribution kit	16
Organizing computer protection	17
Service for registered users	19
Hardware and software requirements	19
INSTALLING AND REMOVING THE APPLICATION	21
Installing the application	21
About ways to install the application	21
Installing the application by using the Setup Wizard	22
Installing the application from the command line	25
Installing the application through the Group Policy Object Editor snap-in	27
Description of setup.ini file settings	27
Initial configuration of the application	30
Upgrading from a previous version of the application	33
About ways to upgrade an old application version	33
Upgrading an old application version through the Group Policy Object Editor snap-in	34
Removing the application	35
About ways to remove the application	35
Removing the application by using the Setup Wizard	35
Removing the application from the command line	37
Removing the application through the Group Policy Object Editor snap-in	37
APPLICATION LICENSING	38
About the End User License Agreement	38
About data submission	38
About the License	39
About activation code	39
About the key file	40
About application activation methods	41
Managing the license	41
Using the Activation Wizard to activate the application	41
Buying a license	42
Renewing a license	42
Viewing license information	42
Activation Wizard	42
APPLICATION INTERFACE	45
Application icon in the taskbar notification area	45

- Application icon context menu46
- Main application window46
- Application settings window48
- STARTING AND STOPPING THE APPLICATION49
 - Enabling and disabling automatic startup of the application49
 - Starting and stopping the application manually49
 - Pausing and resuming computer protection and control50
- PROTECTING THE COMPUTER FILE SYSTEM. FILE ANTI-VIRUS51
 - About File Anti-Virus51
 - Enabling and disabling File Anti-Virus51
 - Automatically pausing File Anti-Virus52
 - Configuring File Anti-Virus53
 - Changing the file security level54
 - Changing the action to take on infected files55
 - Editing the protection scope of File Anti-Virus55
 - Using Heuristic Analyzer with File Anti-Virus56
 - Using scan technologies in the operation of File Anti-Virus57
 - Optimizing file scanning58
 - Scanning compound files58
 - Changing the scan mode59
- SYSTEM WATCHER61
 - About System Watcher61
 - Enabling and disabling System Watcher62
 - Using behavior stream signatures (BSS)63
 - Rolling back malware actions during disinfection63
- EMAIL PROTECTION. MAIL ANTI-VIRUS64
 - About Mail Anti-Virus64
 - Enabling and disabling Mail Anti-Virus64
 - Configuring Mail Anti-Virus65
 - Changing the mail security level67
 - Changing the action to take on infected email messages67
 - Editing the protection scope of Mail Anti-Virus67
 - Scanning compound files that are attached to email messages69
 - Filtering attachments in email messages69
 - Using heuristic analysis70
 - Scanning emails in Microsoft Office Outlook70
 - Scanning emails in The Bat!71
- COMPUTER PROTECTION ON THE INTERNET. WEB ANTI-VIRUS73
 - About Web Anti-Virus73
 - Enabling and disabling Web Anti-Virus73
 - Configuring Web Anti-Virus74
 - Changing the web traffic security level75
 - Changing the action to take on malicious web traffic objects76
 - Scanning URLs against databases of suspicious and phishing web addresses76
 - Using Heuristic Analyzer with Web Anti-Virus77
 - Configuring the duration of caching web traffic78
 - Editing the list of trusted URLs78

PROTECTION OF INSTANT MESSAGING CLIENT TRAFFIC. IM ANTI-VIRUS	80
About IM Anti-Virus.....	80
Enabling and disabling IM Anti-Virus	80
Configuring IM Anti-Virus.....	81
Creating the protection scope of IM Anti-Virus.....	82
Scanning URLs against databases of suspicious and phishing URLs with IM Anti-Virus	82
Using Heuristic Analyzer with IM Anti-Virus	83
NETWORK PROTECTION	84
Firewall	84
About Firewall	84
Enabling or disabling Firewall	85
About network rules	85
About the network connection status	86
Changing the network connection status	86
Managing network packet rules	87
Managing network rules for application groups.....	91
Managing network rules for applications.....	98
Configuring advanced Firewall settings	103
Network Attack Blocker.....	104
About Network Attack Blocker.....	104
Enabling and disabling Network Attack Blocker.....	105
Editing the settings used in blocking an attacking computer.....	106
Monitoring network traffic.....	106
About network traffic monitoring.....	106
Configuring the settings of network traffic monitoring	107
Network Monitor	110
About Network Monitor	110
Starting Network Monitor.....	110
APPLICATION STARTUP CONTROL	111
About Application Startup Control.....	111
Enabling and disabling Application Startup Control.....	111
About Application Startup Control rules.....	113
Managing Application Startup Control rules.....	115
Adding and editing an Application Startup Control rule	115
Adding a trigger condition for an Application Startup Control rule.....	116
Editing the status of an Application Startup Control rule	118
Editing Application Startup Control message templates	119
About Application Startup Control operation modes	120
Switching from Black List mode to White List mode	120
Stage 1. Gathering information about applications that are installed on user computers.....	121
Stage 2. Creating application categories	121
Stage 3. Creating allow rules of Application Startup Control.....	122
Stage 4. Testing allow rules of Application Startup Control	123
Stage 5. Switching to White List mode.....	123
Changing the status of an Application Startup Control rule on the Kaspersky Security Center side	124
APPLICATION PRIVILEGE CONTROL	125
About Application Privilege Control	125

Enabling and disabling Application Privilege Control	126
Placing applications into groups	127
Modifying a trust group	128
Managing Application Control rules	129
Editing control rules for trust groups and application groups.....	129
Editing an application control rule	130
Downloading and updating application control rules from the Kaspersky Security Network database.....	131
Disabling the inheritance of restrictions from the parent process.....	132
Excluding specific application actions from application control rules	133
Configuring storage settings for control rules that govern unused applications	133
Protecting operating system resources and identity data	134
Adding a category of protected resources	134
Adding a protected resource	135
Disabling resource protection.....	136
DEVICE CONTROL	137
About Device Control.....	137
Enabling and disabling Device Control	138
About device and connection bus access rules	139
About trusted devices	139
Standard decisions on access to devices	139
Editing a device access rule	140
Editing a connection bus access rule	141
Actions with trusted devices	142
Adding a device to the list of trusted devices	142
Editing the Users setting of a trusted device	143
Removing a device from the list of trusted devices	143
Editing templates of Device Control messages	144
Obtaining access to a blocked device	144
Creating a device access code.....	146
WEB CONTROL	148
About Web Control	148
Enabling and disabling Web Control.....	149
About web resource access rules.....	150
Actions with web resource access rules	150
Adding and editing a web resource access rule.....	151
Assigning priorities to web resource access rules.....	152
Testing web resource access rules.....	153
Enabling and disabling a web resource access rule	154
Exporting and importing the list of web resource addresses.....	154
Editing masks for web resource addresses	155
Editing templates of Web Control messages	157
UPDATING DATABASES AND APPLICATION SOFTWARE MODULES	159
About database and application module updates	159
About update sources.....	160
Update settings configuration	160
Adding an update source	161
Selecting the update server region	162
Configuring updates from a shared folder.....	162

Selecting the update task run mode.....	164
Starting an update task under the rights of a different user account	165
Starting and stopping an update task	165
Rolling back the last update.....	166
Configuring proxy server settings	166
Enabling and disabling scanning of files in Quarantine after an update	167
SCANNING THE COMPUTER.....	168
About scan tasks	168
Starting or stopping a scan task	169
Configuring scan task settings.....	169
Changing the file security level	171
Changing the action to take on infected files.....	171
Editing the scan scope.....	172
Optimizing file scanning	173
Scanning compound files	174
Selecting the scan method.....	175
Using scan technologies	175
Selecting the scan task run mode	175
Starting a scan task under the account of a different user	176
Scanning removable drives when they are connected to the computer	177
Handling unprocessed files.....	178
About unprocessed files.....	178
Managing the list of unprocessed files	178
VULNERABILITY SCAN	182
About Vulnerability Monitor.....	182
Enabling and disabling Vulnerability Monitor	182
Viewing information about vulnerabilities of running applications	183
About the Vulnerability Scan task	184
Starting or stopping the Vulnerability Scan task	184
Creating the vulnerability scan scope	185
Selecting the Vulnerability Scan task run mode.....	185
Configuring the launch of the Vulnerability Scan task under a different user account	186
Handling detected vulnerabilities	188
About vulnerabilities.....	188
Managing the list of vulnerabilities	189
MANAGING REPORTS	193
Principles of managing reports	193
Configuring report settings.....	194
Configuring the maximum report storage term.....	195
Configuring the maximum size of the report file.....	195
Generating reports.....	195
Viewing reported event information in a separate section	196
Saving a report to file.....	196
Removing information from reports	197
NOTIFICATION SERVICE	199
About Kaspersky Endpoint Security notifications.....	199
Configuring the notification service.....	199

Configuring event log settings.....	200
Configuring delivery of on-screen and email notifications.....	200
Viewing Microsoft Windows Event Log.....	201
MANAGING QUARANTINE AND BACKUP.....	202
About Quarantine and Backup.....	202
Configuring Quarantine and Backup settings.....	203
Configuring the maximum storage term for files in Quarantine and file copies in Backup.....	203
Configuring the maximum size of Quarantine and Backup.....	204
Managing Quarantine.....	204
Moving a file to Quarantine.....	205
Starting a Custom Scan task for files in Quarantine.....	206
Restoring files from Quarantine.....	206
Deleting files from Quarantine.....	207
Sending probably infected files to Kaspersky Lab for examination.....	207
Managing Backup.....	208
Restoring files from Backup.....	208
Deleting backup copies of files from Backup.....	209
ADVANCED APPLICATION SETTINGS.....	210
Trusted zone.....	210
About the trusted zone.....	210
Configuring the trusted zone.....	212
Kaspersky Endpoint Security Self-Defense.....	217
About Kaspersky Endpoint Security Self-Defense.....	217
Enabling or disabling Self-Defense.....	217
Enabling or disabling Remote Control Defense.....	218
Supporting remote administration applications.....	218
Performance of Kaspersky Endpoint Security and compatibility with other applications.....	219
About the performance of Kaspersky Endpoint Security and compatibility with other applications.....	219
Selecting types of detectable threats.....	220
Enabling or disabling Advanced Disinfection technology.....	221
Enabling or disabling energy-saving mode.....	221
Enabling or disabling conceding of resources to other applications.....	222
Password protection.....	223
About restricting access to Kaspersky Endpoint Security.....	223
Enabling and disabling password protection.....	223
Modifying the Kaspersky Endpoint Security access password.....	225
REMOTE ADMINISTRATION THROUGH KASPERSKY SECURITY CENTER.....	226
Managing Kaspersky Endpoint Security.....	226
Starting and stopping Kaspersky Endpoint Security on a client computer.....	226
Configuring Kaspersky Endpoint Security settings.....	227
Managing tasks.....	228
About tasks for Kaspersky Endpoint Security.....	228
Creating a local task.....	229
Creating a group task.....	230
Creating a task for a set of computers.....	230
Starting, stopping, suspending, and resuming a task.....	230
Editing task settings.....	232
Managing policies.....	233

About policies.....	234
Creating a policy	234
Editing policy settings	235
Viewing user complaints in the Kaspersky Security Center event storage	235
PARTICIPATING IN KASPERSKY SECURITY NETWORK	237
About participation in Kaspersky Security Network	237
Enabling and disabling use of Kaspersky Security Network	238
Checking the connection to Kaspersky Security Network.....	238
CONTACTING TECHNICAL SUPPORT	240
How to obtain technical support.....	240
Collecting information for Technical Support	240
Creating a trace file.....	241
Sending data files to the Technical Support server.....	241
Saving data files on the hard drive.....	242
Technical support by phone.....	242
Obtaining technical support via Personal Cabinet	243
GLOSSARY	245
KASPERSKY LAB ZAO	249
INFORMATION ABOUT THIRD-PARTY CODE	250
TRADEMARK NOTICES.....	251
INDEX	252

ABOUT THIS GUIDE

This document is the Administrator Guide for Kaspersky Endpoint Security 8 for Windows (hereafter referred to as Kaspersky Endpoint Security).

This Guide is designed for administrators of local corporate networks and for specialists who are responsible for anti-virus protection of enterprise computers. For regular users whose workplace computers have Kaspersky Endpoint Security installed, this Guide can help to solve to solve certain tasks.

This Guide is intended to do the following:

- Help to install the application on the computer, and to activate and configure it with regard to the user's required tasks.
- Provide a readily searchable source of information for questions related to operation of the application.
- Describe additional sources of information about the application and ways of receiving technical support.

IN THIS SECTION:

In this Guide	10
Document conventions.....	11

IN THIS GUIDE

This Guide comprises the following sections.

Sources of information about the application (see page [13](#))

This section describes sources of information about the application and lists websites that you can use to discuss application operation.

Kaspersky Endpoint Security 8 for Windows (see page [15](#))

This section describes the features of the application and provides brief information about application functions and components. You will learn what items are included in the distribution kit and what services are available for registered users of the application. This section provides information about the software and hardware requirements that a computer must meet to allow installation.

Installing and removing the application (see page [21](#))

This section guides you through installing Kaspersky Endpoint Security on your computer, completing initial configuration, upgrading from a previous version of the application, and removing the application from the computer.

Application licensing (see page [38](#))

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the types of licenses, the ways to activate the application, and renew your license.

Application interface (see page [45](#))

This section describes the basic elements of the graphical interface of the application: the application icon and its context menu, main application window, and application settings window.

Starting and stopping the application (see page [49](#))

This section describes how you can configure automatic startup of the application, start or stop the application manually, and pause or resume protection and control components.

Typical tasks (see the section "Protecting the computer file system. File Anti-Virus" on page [51](#))

A group of sections that describe typical tasks and application components. Those sections provide detailed information about how to configure tasks and application components.

Remote administration through Kaspersky Security Center (see page [226](#))

This section describes Kaspersky Endpoint Security administration through Kaspersky Security Center.

Participating in Kaspersky Security Network (see page [237](#))

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

Contacting Technical Support (see page [240](#))

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

Glossary (see page [245](#))

This section contains a list of terms that are mentioned in the document and their definitions.

Kaspersky Lab ZAO (see page [249](#))

This section provides information about Kaspersky Lab ZAO.

Index

This section allows you to quickly find required information within the document.

DOCUMENT CONVENTIONS

The document text is accompanied by semantic elements to which we recommend paying particular attention: warnings, hints, and examples.

Document conventions are used to highlight semantic elements. The following table shows document conventions and examples of their use.

Table 1. Document conventions

Sample text	Description of document convention
Note that ...	Warnings are highlighted in red and boxed. Warnings provide information about possible unwanted actions that may lead to data loss or failures in computer operation.
It is recommended to use...	Notes are boxed. Notes provide auxiliary and reference information. Notes may contain useful hints, recommendations, specific values, or important special cases in operation of the application.
Example: ...	Examples are listed in respective sections under the heading "Example".
<i>Update</i> means... The <i>Databases are out of date</i> event occurs.	The following semantic elements are italicized in the text: <ul style="list-style-type: none"> • New terms • Names of application statuses and events
Press ENTER . Press Option+N .	Names of keyboard keys appear in bold and are capitalized. Names of keys that are connected by a + (plus) sign indicate the use of a key combination. Those keys must be pressed simultaneously.
Click the Enable button.	Names of application interface elements, such as entry fields, menu items, and buttons, are set off in bold.
➡ <i>To create a trace file:</i>	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
In the command line, enter the following text: <code>kav update</code> The following message then appears: Specify the date in <code>dd:mm:yy</code> format.	The following types of text content are set off with a special font (Courier): <ul style="list-style-type: none"> • Text in the command line • Text of messages that the application displays on screen • Data that the user must enter.
<IP address of your computer>	Variables are enclosed in angle brackets. Each of the variables should be replaced by the corresponding value, omitting angle brackets.

SOURCES OF INFORMATION ABOUT THE APPLICATION

This section describes sources of information about the application and lists websites that you can use to discuss application operation.

You can select the most suitable information source, depending on the level of importance and urgency of the issue.

IN THIS SECTION:

Sources of information for independent research.....	13
Discussing Kaspersky Lab applications on the Forum	14
Contacting the Documentation Development Team by email.....	14

SOURCES OF INFORMATION FOR INDEPENDENT RESEARCH

You can use the following sources to independently find information about the application:

- Application page on the Kaspersky Lab website
- Page on the Kaspersky Lab Technical Support (hereafter also "Technical Support") website (Knowledge Base)
- Online help
- Documentation

If you cannot find a solution for your issue, we recommend that you contact Kaspersky Lab Technical Support (see the section "Technical support by phone" on page [242](#)).

An Internet connection is required to use information sources on the Kaspersky Lab website.

Application page on the Kaspersky Lab website

The Kaspersky Lab website features an individual page for each application.

On the page <http://www.kaspersky.com/endpoint-security-windows>, you can view general information about the application, its functions, and its features.

The page <http://www.kaspersky.com> contains a link to the eStore. There you can purchase or renew the application.

Application page on the Technical Support website (Knowledge Base)

Knowledge Base is a section on the Technical Support website that provides advice on using Kaspersky Lab applications. Knowledge Base comprises reference articles that are grouped by topic.

On the page of the application in the Knowledge Base, you can read articles that provide useful information, recommendations, and answers to frequently asked questions on how to purchase, install, and use Kaspersky Endpoint Security for workstations <http://support.kaspersky.com/kes8wks> and for file servers <http://support.kaspersky.com/kes8fs>.

Articles may provide answers to questions relating not just to Kaspersky Endpoint Security, but also to other Kaspersky Lab applications. They also may contain news from Technical Support.

Online help

The online help of the application comprises help files.

Context help provides information about each window of the application, listing and describing the corresponding settings and a list of tasks.

Full help provides detailed information about how to manage computer protection by using the application.

Administrator Guide

You can download the Administrator Guide in PDF format from the **Download** section on the Kaspersky Lab website. Consult this document for help with installing and activating the application on the computers of a local area network and with configuring application settings. The document provides detailed information about how to manage computer protection by using the application.

DISCUSSING KASPERSKY LAB APPLICATIONS ON THE FORUM

If your question does not require an urgent answer, you can discuss it with Kaspersky Lab specialists and other users on our Forum (<http://forum.kaspersky.com/index.php?showforum=5>).

In this forum you can view existing topics, leave your comments, and create new discussion topics.

CONTACTING THE DOCUMENTATION DEVELOPMENT TEAM BY EMAIL

To contact the Documentation Development Team, send an email. In the email subject line, type "Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Windows".

KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS

This section describes the features of the application and provides brief information about application functions and components. You will learn what items are included in the distribution kit and what services are available for registered users of the application. This section provides information about the software and hardware requirements that a computer must meet to allow installation.

IN THIS SECTION:

What's new.....	15
Distribution kit.....	16
Organizing computer protection	16
Service for registered users	19
Hardware and software requirements	19

WHAT'S NEW

Kaspersky Endpoint Security 8 for Windows offers the following new features:

- The Application Control functionality has been added, which lets you allow or block startup of individual applications depending on the policy of the IT department of your company. Application Control comprises the following components:
 - **Application Startup Control**, which operates on the basis of allow and block rules that are specified by the administrator of the local area network. Rules can be created on the basis of software categories that are provided by Kaspersky Lab or conditions that are specified by the administrator of the local area network. Thanks to integration with Active Directory®, the rules that allow or block startup of applications are specified for Active Directory users and user groups.
 - **Application Privilege Control**, which blocks application activity depending on the level of application danger and reputation information. Information on the reputation of applications is provided by Kaspersky Lab.
 - **Vulnerability Monitor**, which detects vulnerabilities both in applications that are started on the computer and in all applications that are installed on the computer.
- The Web Control component has been added, which lets you restrict or block user access to web resources according to rules. Categories of web content, data types, and individual web addresses or their groups can be specified as rule parameters. Thanks to integration with Active Directory, web access rules are defined for Active Directory users and user groups.
- New main application window interface: the main window shows statistics about the operation of control and protection components and the performance of update and scan tasks.

Improvements:

- Enhanced anti-virus protection, including through integration with Kaspersky Security Network. Integration with Kaspersky Security Network provides information about file and web address reputations.

- Improved advanced disinfection technology.
- Improved self-defense technology against changes to application files, memory processes, and system registry values.
- Improved proactive defense technology:
 - The System Watcher component logs application activity.
 - The BSS (Behavior Stream Signatures) proactive defense technology detects malicious behavior based on regularly updated signatures.
 - You can now roll back malicious actions of applications during disinfection.
- The Firewall component has been improved, letting you monitor inbound and outbound traffic across ports, IP addresses, and applications that generate traffic.
- The Intrusion Detection System (IDS) technology has been improved, with the addition of support for exclusions that are specified by using IP addresses.
- The Device Control component has been improved:
 - Sets of supported buses and device types have been expanded.
 - Device serial numbers can now be used as criteria.
 - It is now possible to restrict access to devices with file systems at the level of reading / writing.
 - It is now possible to set a schedule for users' access to devices.
 - Integration with Active Directory has been added.
- Scanning of traffic over the IRC, Mail.ru, and AIM® protocols has been added.

DISTRIBUTION KIT

Kaspersky Endpoint Security is distributed through online stores of Kaspersky Lab (for example, <http://www.kaspersky.com>, in the **eStore** section) or partner companies.

The distribution kit contains the following items:

- Files that are required for installing the application in any of the available ways (see the section "About ways to install the application" on page [21](#)).
- The file ksn.txt, in which you can read through the terms of participation in Kaspersky Security Network (see the section "Participating in Kaspersky Security Network" on page [237](#)).
- The file license.txt, which you can view to look through the License Agreement. The License Agreement specifies the terms of use of the application.

Information that is required for application activation is sent to you by email after payment.

For more details on purchase methods and the distribution kit, contact the Sales Department.

ORGANIZING COMPUTER PROTECTION

Kaspersky Endpoint Security provides comprehensive computer protection against known and new threats, network and phishing attacks, and other unwanted content.

Each type of threat is handled by a dedicated component. Components can be enabled or disabled independently of one another, and their settings can be configured.

In addition to the real-time protection that the application components provide, we recommend that you regularly *scan* the computer for viruses and other threats. This helps to rule out the possibility of spreading malware that is undetected by protection components due to a low security level setting or for other reasons.

To keep Kaspersky Endpoint Security up to date, you must *update* the databases and modules that the application uses. The application is updated automatically by default, but if necessary, you can update the databases and application modules manually.

The following application components are control components:

- **Application Startup Control.** This component keeps track of user attempts to start applications and regulates the startup of applications.
- **Application Privilege Control.** This component registers the actions of applications in the operating system and regulates application activity depending on the trust group of a particular application. A set of rules is specified for each group of applications. These rules regulate the access of applications to user data and to resources of the operating system. Such data includes user files (**My Documents** folder, cookies, user activity information) and files, folders, and registry keys that contain settings and important information from the most frequently used applications.
- **Vulnerability Monitor.** The Vulnerability Monitor component runs a real-time vulnerability scan of applications that are started or are running on the user's computer.
- **Device Control.** This component lets you set flexible restrictions on access to data storage devices (such as hard drives, removable media, tape drives, and CDs and DVDs), data transmission equipment (such as modems), equipment that converts information into hard copies (such as printers), or interfaces for connecting devices to computers (such as USB, Bluetooth, and Infrared).
- **Web Control.** This component lets you set flexible restrictions on access to web resources for different user groups.

The operation of control components is based on the following rules:

- Application Startup Control uses application startup control rules (see the section "About Application Startup Control rules" on page [113](#)).
- Application Privilege Control uses application control rules (see the section "About Application Privilege Control" on page [125](#)).
- Device Control uses device access rules and connection bus access rules (see the section "About device and connection bus access rules" on page [139](#)).
- Web Control uses web resource access rules (see the section "About web resource access rules" on page [150](#)).

The following application components are protection components:

- **File Anti-Virus.** This component protects the file system of the computer from infection. File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on the computer and on all connected drives. File Anti-Virus intercepts every attempt to access a file and scans the file for viruses and other threats.
- **System Watcher.** This component keeps a record of application activity on the computer and provides this information to other components to ensure more effective protection.

- **Mail Anti-Virus.** This component scans incoming and outgoing email messages for viruses and other threats.
- **Web Anti-Virus.** This component scans traffic that arrives on the user's computer via the HTTP and FTP protocols, and checks whether URLs are listed as suspicious or phishing web addresses.
- **IM Anti-Virus.** This component scans traffic that arrives on the computer via instant messaging protocols. It ensures the safe operation of numerous instant messaging applications.
- **Firewall.** This component protects personal data that is stored on the computer and blocks all kinds of threats to the operating system while the computer is connected to the Internet or to a local area network. The component filters all network activity according to two types of rules: application network rules and network packet rules (see the section "About network rules" on page [85](#)).
- **Network Monitor.** This component lets you view network activity of the computer in real time.
- **Network Attack Blocker.** This component inspects inbound network traffic for activity that is typical of network attacks. On detecting an attempted network attack that targets your computer, Kaspersky Endpoint Security blocks network activity from the attacking computer.

The following tasks are provided in Kaspersky Endpoint Security:

- **Full Scan.** Kaspersky Endpoint Security thoroughly scans the operating system, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.
- **Custom Scan.** Kaspersky Endpoint Security scans the objects that are selected by the user.
- **Critical Areas Scan.** Kaspersky Endpoint Security scans objects that are loaded at operating system startup, RAM, and objects that are targeted by rootkits.
- **Update.** Kaspersky Endpoint Security downloads updated application databases and modules. Updating keeps the computer protected against new viruses and other threats at all times.
- **Vulnerability Scan.** Kaspersky Endpoint Security scans the operating system and installed software for vulnerabilities. This scanning ensures timely detection and removal of potential problems that intruders can exploit.

Remote administration through Kaspersky Security Center

Kaspersky Security Center makes it possible to remotely start and stop Kaspersky Endpoint Security on a client computer, and to remotely manage and configure application settings.

Service functions and applications

Kaspersky Endpoint Security comes with a number of service functions. Service functions are meant to keep the application up to date, expand its functionality, and assist the user with operating it.

- **Reports.** In the course of its operation, the application keeps a report on each application component and task. The report contains a list of Kaspersky Endpoint Security events and all operations that the application performs. In case of an incident, you can send reports to Kaspersky Lab, where Technical Support specialists can look into the issue in more detail.
- **Data storage.** If the application detects infected or probably infected files while scanning the computer for viruses and other threats, it blocks those files. Kaspersky Endpoint Security moves probably infected files to a special storage called *Quarantine*. Kaspersky Endpoint Security stores copies of disinfected and deleted files in *Backup*. Kaspersky Endpoint Security moves files that are not processed for any reason to the *list of unprocessed files*. You can scan files, restore files to their original folders, manually move files to Quarantine, and empty the data storage.
- **Notification service.** The notification service keeps the user informed about the current protection status of the computer and the operation of Kaspersky Endpoint Security. Notifications can be displayed on the screen or sent by email.

- **Kaspersky Security Network.** User participation in Kaspersky Security Network enhances the effectiveness of computer protection through real-time collection of information on the reputation of files, web resources, and software from users worldwide.
- **License.** Using a license unlocks full application functionality, provides access to application database and module updates, detailed information about the application, and assistance from Kaspersky Lab Technical Support.
- **Support.** All registered users of Kaspersky Endpoint Security can contact Technical Support specialists for assistance. You can send a request from Personal Cabinet on the Technical Support website or receive assistance from support personnel over the phone.

SERVICE FOR REGISTERED USERS

By purchasing a user license for the application, you become a registered user of Kaspersky Lab applications and can benefit from the following services during the entire validity term of the license:

- Database updates and access to new versions of the application
- Consultations by phone and by email on issues that are related to installation, configuration, and use of the application
- Notifications about the release of new applications by Kaspersky Lab and of new viruses. To use this service, subscribe to news delivery from Kaspersky Lab on the Technical Support website.

No consultations are provided on issues that are related to the functioning of operating systems or third-party software and technologies.

HARDWARE AND SOFTWARE REQUIREMENTS

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

General requirements:

- 1 GB of free disk space on the hard drive
- CD/DVD-ROM (for installing the application from a retail installation CD)
- Microsoft® Internet Explorer® 7.0 or later
- Microsoft Windows Installer 3.0 or later
- An Internet connection for activating the application and updating application databases and modules

Hardware requirements for computers with workstation operating systems installed:

- Microsoft Windows XP Professional SP3, Microsoft Windows XP Professional x64 Edition SP2:
 - Intel® Pentium® 1 GHz or faster processor (or compatible equivalent)
 - 256 MB of free RAM
- Microsoft Windows 7 Professional / Enterprise / Ultimate (SP0 or later), Microsoft Windows 7 Professional / Enterprise / Ultimate (x64 Edition SP0 or later), Microsoft Windows Vista® SP2, Microsoft Windows Vista x64 Edition SP2:
 - Intel Pentium 2 GHz processor or faster (or compatible equivalent)

- 512 MB of free RAM
- Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows Embedded Standard 7 x64 Edition SP1, Microsoft Windows Embedded POSReady 2009 latest SP:
 - Intel Pentium 800 GHz processor or faster (or compatible equivalent)
 - 256 MB of free RAM

Hardware requirements for computers with file server operating systems installed:

Microsoft Windows Small Business Server 2008 Standard x64 Edition, Microsoft Windows Small Business Server 2011 Essentials / Standard (x64 Edition), Microsoft Windows Server® 2008 R2 Standard / Enterprise (x64 Edition SP1), Microsoft Windows Server 2008 Standard / Enterprise SP2, Microsoft Windows Server 2008 Standard / Enterprise SP2 (x64 Edition), Microsoft Windows Server 2003 R2 Standard / Enterprise SP2, Microsoft Windows Server 2003 R2 Standard x64 Edition SP2, Microsoft Windows Server 2003 Standard SP2, Microsoft Windows Server 2003 Standard x64 Edition SP2:

- Intel Pentium 2 GHz processor or faster (or compatible equivalent)
- 512 MB of free RAM

INSTALLING AND REMOVING THE APPLICATION

This section guides you through installing Kaspersky Endpoint Security on your computer, completing initial configuration, upgrading from a previous version of the application, and removing the application from the computer.

IN THIS SECTION:

Installing the application	21
Upgrading from a previous version of the application	33
Removing the application	35

INSTALLING THE APPLICATION

This section describes how to install Kaspersky Endpoint Security on your computer and complete initial configuration of the application.

IN THIS SECTION:

About ways to install the application	21
Installing the application by using the Setup Wizard	22
Installing the application from the command line.....	25
Installing the application through the Group Policy Object Editor snap-in	27
Description of setup.ini file settings	27
Initial configuration of the application	30

ABOUT WAYS TO INSTALL THE APPLICATION

There are several ways to install Kaspersky Endpoint Security 8 for Windows on a computer:

- *Local installation* – the application is installed on an individual computer. Starting and completing a local installation requires direct access to the computer. A local installation can be performed in one of two modes:
 - *Interactive*, by using the Setup Wizard (see the section "Installing the application by using the Setup Wizard" on page [22](#)). This mode requires your involvement in the setup process.
 - *Silent*, in which case application installation is started from the command line and does not require your involvement in the setup process (see the section "Installing the application from the command line" on page [25](#)).
- *Remote installation* – installation on a computer within a network, performed remotely from the administrator's workstation by using:

- Kaspersky Security Center software complex (see "Kaspersky Security Center Deployment Guide")
- group domain policies of Microsoft Windows Server (see the section "Installing the application through the Group Policy Object Editor snap-in" on page [27](#)).

We recommend closing all active applications before starting the installation of Kaspersky Endpoint Security (including remote installation).

INSTALLING THE APPLICATION BY USING THE SETUP WIZARD

The interface of the Setup Wizard consists of a sequence of pages (steps). You can navigate between the Setup Wizard pages by using the **Back** and **Next** buttons. To close the Setup Wizard after it completes its task, click the **Finish** button. To stop the Setup Wizard at any stage, click the **Cancel** button.

➔ *To install the application or upgrade the application from a previous version by using the Setup Wizard:*

1. Start the setup.exe file.
The Setup Wizard starts.
2. Follow the instructions of the Setup Wizard.

IN THIS SECTION:

Step 1. Making sure that the computer meets installation requirements	22
Step 2. Welcome page of the installation procedure	23
Step 3. Reviewing the License Agreement.....	23
Step 4. Kaspersky Security Network Data Collection Statement.....	23
Step 5. Selecting the installation type	23
Step 6. Selecting application components to install	24
Step 7. Selecting the destination folder	24
Step 8. Adding exclusions from virus scanning	24
Step 9. Preparing for application installation	25
Step 10. Installing the application.....	25

STEP 1. MAKING SURE THAT THE COMPUTER MEETS INSTALLATION REQUIREMENTS

Before installing Kaspersky Endpoint Security 8 for Windows on a computer or updating a previous version of the application, the following conditions are checked:

- Whether the operating system and the Service Pack meet the software requirements for installation (see the section "Hardware and software requirements" on page [19](#)).
- Whether the hardware and software requirements are met (see the section "Hardware and software requirements" on page [19](#)).

- Whether the user has the rights to install the software product

If any one of the previous requirements is not met, a relevant notification is displayed on the screen.

If the computer meets the above-listed requirements, the Setup Wizard searches for Kaspersky Lab applications that may lead to conflicts when running at the same time as Kaspersky Endpoint Security. If such applications are found, you are prompted to remove them manually.

If the detected applications include Kaspersky Anti-Virus 6.0 for Windows Workstations® MP3 / MP4 or Kaspersky Anti-Virus 6.0 for Windows Servers MP3 / MP4, all data that can be migrated (such as activation details and application settings) is preserved and used during the installation of Kaspersky Endpoint Security 8 for Windows. However, Kaspersky Anti-Virus 6.0 for Windows Workstations MP3 / MP4 or Kaspersky Anti-Virus 6.0 for Windows Servers MP3 / MP4 is removed automatically.

STEP 2. WELCOME PAGE OF THE INSTALLATION PROCEDURE

If the operating system on which you are installing Kaspersky Endpoint Security 8 for Windows fully meets the requirements, a welcome page appears after you start the installation package. The welcome page notifies you of the beginning of installation of Kaspersky Endpoint Security 8 for Windows on the computer.

To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 3. REVIEWING THE LICENSE AGREEMENT

During this step, you are advised to review the license agreement between you and Kaspersky Lab.

Carefully review the agreement and, if you agree with all of its terms, select the **I accept the terms of the License Agreement** check box.

To return to the previous step of the Setup Wizard, click the **Back** button. To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 4. KASPERSKY SECURITY NETWORK DATA COLLECTION STATEMENT

During this step, you are invited to participate in Kaspersky Security Network.

Review the Kaspersky Security Network Data Collection Statement:

- If you accept all of the terms, on the Setup Wizard page, select the option **I agree to participate in Kaspersky Security Network**.
- If you do not accept the conditions of participation in Kaspersky Security Network, on the Setup Wizard page, select the option **I do not agree to participate in Kaspersky Security Network**.

To return to the previous step of the Setup Wizard, click the **Back** button. To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 5. SELECTING THE INSTALLATION TYPE

During this step, you can select the most suitable installation type of Kaspersky Endpoint Security 8 for Windows:

- *Full installation.* If you select this type of installation, the application is installed in its entirety, with the protection settings that are recommended by Kaspersky Lab.
- *Custom installation.* If you select this type of installation, you are offered to select the components to be installed (see the section "Step 6. Selecting application components to install" on page [24](#)) and specify the destination folder for installing the application (see the section "Step 7. Selecting the destination folder" on page [24](#)).

To return to the previous step of the Setup Wizard, click the **Back** button. To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 6. SELECTING APPLICATION COMPONENTS TO INSTALL

This step is performed if you select *Custom installation* of the application.

During this step, you can select the Kaspersky Endpoint Security 8 for Windows components that you want to install. All application components are selected for installation by default.

To select a component that you want to install, click the icon next to the component name to bring up the context menu. Then select **Component will be installed on the local hard drive**. For more details on what tasks are performed by the selected component and how much disk space is required to install the component, refer to the lower part of the current Setup Wizard page.

To view detailed information about the available space on local hard drives, click the **Disk** button. Information is shown in the **Available disk space** window that opens.

To cancel component installation, in the context menu, select the **Component will be unavailable** option.

To return to the list of default components, click the **Reset** button.

To return to the previous step of the Setup Wizard, click the **Back** button. To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 7. SELECTING THE DESTINATION FOLDER

This step is available if you select *Custom installation* of the application.

During this step, you can specify the path to the destination folder where the application will be installed. To select the destination folder for the application, click the **Browse** button.

To view information about available space on local hard drives, click the **Disk** button. Information is shown in the **Available disk space** window that opens.

To return to the previous step of the Setup Wizard, click the **Back** button. To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 8. ADDING EXCLUSIONS FROM VIRUS SCANNING

This step is available if you select *Custom installation* of the application.

At this stage you can specify which exclusions from virus scanning you want to add to the application settings.

The **Exclude areas that are recommended by Microsoft from virus scan scope / Exclude areas that are recommended by Kaspersky Lab from virus scan scope** check boxes exclude, respectively, areas that are recommended by Microsoft or Kaspersky Lab from the trusted zone or includes them.

If one of these check boxes is selected, Kaspersky Endpoint Security includes, respectively, the areas that Microsoft or Kaspersky Lab recommends in the trusted zone. Kaspersky Endpoint Security does not scan such areas for viruses and other threats.

The **Exclude areas recommended by Microsoft / Kaspersky Lab from virus scanning** check box is available when Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers.

To return to the previous step of the Setup Wizard, click the **Back** button. To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 9. PREPARING FOR APPLICATION INSTALLATION

Because your computer may be infected with malicious programs that could interfere with installation of Kaspersky Endpoint Security 8 for Windows, you are advised to protect the installation process.

Installation process protection is enabled by default.

If the application cannot be installed (for example, when performing remote installation with the help of Windows Remote Desktop), you are advised to disable protection of the installation process. The inability to install may be because protection of application installation is enabled. If this happens, abort the installation, and quit and start the Setup Wizard from the beginning. At step 8 (Preparing for application installation), clear the **Secure installation process** check box.

The **Add path to avp.com file to %PATH% system variable** check box enables / disables an option that adds the path to the avp.com file to the %PATH% system variable.

If the check box is selected, starting Kaspersky Endpoint Security or any of its tasks from the command line does not require entering the path to the executable file. It is enough to enter the name of the executable file and the command to start a particular task.

To return to the previous step of the Setup Wizard, click the **Back** button. To install the program, click the **Install** button. To stop the Setup Wizard, click the **Cancel** button.

Current network connections may be terminated while the application is being installed on the computer. Most terminated connections are restored after a short time.

STEP 10. INSTALLING THE APPLICATION

Installation of the application can take some time. Wait for it to complete.

If you are updating a previous version of the application, this step also includes settings migration and removal of the previous version of the application.

After installation of Kaspersky Endpoint Security 8 for Windows is completed, the Initial Configuration Wizard starts (see the section "Initial configuration of the application" on page [30](#)).

INSTALLING THE APPLICATION FROM THE COMMAND LINE

➤ *To start the Setup Wizard from the command line,*

type the following string in the command line: `setup.exe` or `msiexec /i <installation package name>`.

➤ *To install the application or upgrade from a previous version of the application in non-interactive mode (without starting the Setup Wizard),*

type the following string in the command line: `setup.exe /pEULA=1 /pKSN=1|0 /pALLOWREBOOT=1|0 /s` or

`msiexec /i <installation package name> EULA=1 KSN=1|0 ALLOWREBOOT=1|0 /qn,`

where:

- `EULA=1` means that you accept the terms of the license agreement. The text of the License Agreement is included in the distribution kit of Kaspersky Endpoint Security 8 for Windows (see the section "Distribution kit" on page [16](#)). Accepting the terms of the License Agreement is necessary for installing the application or updating a previous version of the application.

- `KSN=1|0` signifies agreement or refusal to participate in Kaspersky Security Network (also referred to as KSN). This parameter is not required. If the value of the `KSN` parameter is not specified in the command string, it is assumed by default that you refuse to participate in KSN. The text of the KSN participation policy is included in the distribution kit of Kaspersky Endpoint Security 8 for Windows (see the section "Distribution kit" on page [16](#)).
- `ALLOWREBOOT=1|0` signifies agreement or refusal to allow an automatic restart of the computer, if this is required, after installation of the application or an upgrade from a previous version of the application. This parameter is not required. If no value of the `ALLOWREBOOT` parameter is specified in the command string, it is assumed by default that you do not allow automatic restart of the computer after installation of the application or an upgrade from a previous version of the application.

A restart of the computer may be required after an upgrade from a previous version of the application, or when Kaspersky Endpoint Security detects and removes third-party anti-virus software during installation.

The computer can be restarted automatically only in non-interactive installation mode (with the `/qn` key).

- ➔ *To install the application or upgrade from a previous version of the application with a password that authorizes changes to application settings and operations with the application,*

type the following string in the command line:

- `setup.exe /pKLPASSWD=***** /pKLPASSWDAREA=<password scope>` or
`msiexec /i <installation package name> KLPASSWD=***** KLPASSWDAREA=<password scope>` to install the application or upgrade from a previous version of the application in interactive mode.
- `setup.exe /pEULA=1 /pKSN=1|0 /pKLPASSWD=***** /pKLPASSWDAREA=<password scope> /s` or
`msiexec /i <installer package name> EULA=1 KSN=1|0 KLPASSWD=***** KLPASSWDAREA=<password scope> ALLOWREBOOT=1|0/qn` to install the application or upgrade from a previous version of the application in non-interactive mode.

In this command string, one or more of the following values of the `KLPASSWDAREA` parameter can be specified instead of `<password area>`, separated with a ";":

- `SET`. Set a password for editing application settings.
- `EXIT`. Set a password for exiting the application.
- `DISPROTECT`. Set a password for disabling protection components and stopping scan tasks.
- `DISPOLICY`. Set a password for disabling the Kaspersky Security Center policy.
- `UNINST`. Set a password for removing the application from the computer.
- `DISCTRL`. Set a password for disabling control components (Application Startup Control, Application Privilege Control, Vulnerability Monitor, Device Control, Web Control).
- `REMOVELIC`. Set a password for deleting the application license.

The use of the following files is supported when you install the application or upgrade from a previous version of the application:

- `setup.ini` (see the section "Description of setup.ini file settings" on page [27](#)), which contains general application setup settings
- `install.cfg` configuration file
- `setup.reg`

The setup.ini, install.cfg, and setup.reg files must be located in the same folder as the Kaspersky Endpoint Security 8 for Windows installation package.

INSTALLING THE APPLICATION THROUGH THE GROUP POLICY OBJECT EDITOR SNAP-IN

The Group Policy Object Editor snap-in lets you install Kaspersky Endpoint Security on enterprise workstations that belong to a domain, without using Kaspersky Security Center.

➔ *To install Kaspersky Endpoint Security through the Group Policy Object Editor snap-in:*

1. Create a shared network folder on a computer that acts as domain controller.
2. Place the MSI installation package for the new version of Kaspersky Endpoint Security in the shared network folder that you created during the previous step.

In addition, you can copy the setup.ini file to this shared network folder (see the section "Description of setup.ini file settings" on page [27](#)), which contains general Kaspersky Endpoint Security setup settings, along with the install.cfg configuration file and the key file.

3. Open the Group Policy Object Editor snap-in through the MMC console (see the *Microsoft Windows Server help files* for detailed instructions on using the Editor).
4. Create a new installation package of the Group Policy Object Editor snap-in. To do so:
 - a. In the console tree, select **Group Policy Object** → **Computer Configuration** → **Software Settings** → **Software installation**.
 - b. Right-click to bring up the context menu of the **Software installation** node.
 - c. In the context menu, select **New** → **Package**.

The standard **Open** window of Microsoft Windows Server opens.
 - d. In the standard **Open** window of Microsoft Windows Server, specify the path to the MSI installation package of Kaspersky Endpoint Security.
 - e. In the **Deploy Software** window, select **Assigned**.
 - f. Click **OK**.

The group policy is enforced on each workstation the next time that the computer is registered in the domain. Kaspersky Endpoint Security is then installed on all computers within the domain.

DESCRIPTION OF SETUP.INI FILE SETTINGS

The setup.ini file is used when installing the application from the command line or from the Group Policy Object Editor snap-in. The setup.ini file is located in the folder of the Kaspersky Endpoint Security installation package.

The setup.ini file contains the following settings:

[Setup] – general application installation settings:

- `InstallDir` – path to the application installation folder
- `ActivationCode` – Kaspersky Endpoint Security activation code

- `Eula` – acceptance or rejection of the terms of the End User License Agreement. Possible values of the `Eula` parameter:
 - 1. Specifying this value signifies acceptance of the terms of the License Agreement.
 - 0. Specifying this value signifies rejection of the terms of the License Agreement.
- `KSN` – agreement or refusal to participate in Kaspersky Security Network. Possible values of the `KSN` parameter:
 - 1. Specifying this value signifies agreement to participate in Kaspersky Security Network.
 - 0. Specifying this value signifies refusal to participate in Kaspersky Security Network.
- `Password` – set password for accessing the administration of Kaspersky Endpoint Security options and settings
- `PasswordArea` – specify the area that is covered by the password for accessing the administration of Kaspersky Endpoint Security options and settings Possible values of the `PasswordArea` parameter:
 - `SET`. Set a password for editing application settings.
 - `EXIT`. Set a password for exiting the application.
 - `DISPROTECT`. Set a password for disabling protection components and stopping scan tasks.
 - `DISPOLICY`. Set a password for disabling the Kaspersky Security Center policy.
 - `UNINST`. Set a password for removing the application from the computer.
 - `DISCTRL`. Set a password for disabling control components (Application Startup Control, Application Privilege Control, Vulnerability Monitor, Device Control, Web Control).
 - `REMOVELIC`. Set a password for deleting the application license.
- `SelfProtection` – enable or disable Kaspersky Endpoint Security Self-Defense during installation. Possible values of the `SelfProtection` parameter:
 - 1. Specifying this value signifies that Self-Defense will be enabled.
 - 0. Specifying this value signifies that Self-Defense will be disabled.
- `Reboot` – whether to restart the computer after installation of the application, if a restart is required. Possible values of the `Reboot` parameter:
 - 1. Specifying this value signifies that the computer will be restarted, if necessary, after the application is installed.
 - 0. Specifying this value signifies that the computer will not be restarted after the application is installed.
- `MSExclusions` – add applications recommended by Microsoft to exclusions from scanning. This setting is available only for file servers that run on Microsoft Windows Server (see the section "Hardware and software requirements" on page [19](#)). Possible values of the `MSExclusions` parameter:
 - 1. Specifying this value signifies that applications recommended by Microsoft will be added to exclusions from scanning.
 - 0. Specifying this value signifies that applications recommended by Microsoft will not be added to exclusions from scanning.

- `KLExclusions` – add applications recommended by Kaspersky Lab to exclusions from scanning. Possible values of the `KLExclusions` parameter:
 - 1. Specifying this value signifies that applications recommended by Kaspersky Lab will be added to exclusions from scanning.
 - 0. Specifying this value signifies that applications recommended by Kaspersky Lab will not be added to exclusions from scanning.
- `NoKLIM5` – whether to enable the installation of Kaspersky Endpoint Security network drivers during installation of the application. The network drivers are installed by default. Kaspersky Endpoint Security network drivers, which belong to the group of NDIS drivers and are responsible for intercepting network traffic for such application components as Device Control, Web Control, Mail Anti-Virus, Web Anti-Virus, Firewall, and Network Attack Blocker, may cause conflicts with other applications or equipment that is installed on the computer. To prevent possible conflicts, you may choose not to install network drivers on computers that run on Microsoft Windows XP Professional x86 or on Microsoft Windows Server 2003 x86. Possible values of the `NoKLIM5` parameter:
 - 1. Specifying this value disables installation of Kaspersky Endpoint Security network drivers during application installation.
 - 0. Specifying this value enables installation of Kaspersky Endpoint Security network drivers during application installation.
- `AddEnvironment` – whether to supplement the `%PATH%` system variable with the path to executable files that are located in the Kaspersky Endpoint Security setup folder. Possible values of the `AddEnvironment` parameter:
 - 1. Specifying this value signifies that the `%PATH%` system variable will be supplemented with the path to executable files that are located in the Kaspersky Endpoint Security setup folder.
 - 0. Specifying this value signifies that the `%PATH%` system variable will not be supplemented with the path to executable files that are located in the Kaspersky Endpoint Security setup folder.

[Components] – selection of application components to be installed. If none of the components are specified, all components that are available for the operating system are installed.

- `ALL` – installation of all components.
- `MailAntiVirus` – installation of the Mail Anti-Virus component.
- `FileAntiVirus` – installation of the File Anti-Virus component.
- `IMAntiVirus` – installation of the IM Anti-Virus component.
- `WebAntiVirus` – installation of the Web Anti-Virus component.
- `ApplicationPrivilegeControl` – installation of the Application Privilege Control component.
- `SystemWatcher` – installation of the System Watcher component.
- `Firewall` – installation of the Firewall component.
- `NetworkAttackBlocker` – installation of the Network Attack Blocker component.
- `WebControl` – installation of the Web Control component.
- `DeviceControl` – installation of the Device Control component.
- `ApplicationStartupControl` – installation of the Application Startup Control component.

- `VulnerabilityAssessment` – installation of vulnerability scan functionality.
- `AdminKitConnector` – installation of Administration Kit Connector for remote administration of the application through Kaspersky Security Center.

Possible parameter values:

- 1. Specifying this value signifies that the component will be installed.
- 0. Specifying this value signifies that the component will not be installed.

[Tasks] – selection of tasks to be included in the list of Kaspersky Endpoint Security tasks. If no task is specified, all tasks are included in the task list of Kaspersky Endpoint Security.

- `ScanMyComputer` – Full Scan task.
- `ScanCritical` – Critical Areas Scan task.
- `Updater` – Update task.

Possible parameter values:

- 1. Specifying this value signifies that the update task will be included in the list of Kaspersky Endpoint Security tasks.
- 0. Specifying this value signifies that the update task will not be included in the list of Kaspersky Endpoint Security tasks.

The alternatives to the value 1 are the values `yes`, `on`, `enable`, and `enabled`. The alternatives to the value 0 are the values `no`, `off`, `disable`, and `disabled`.

INITIAL CONFIGURATION OF THE APPLICATION

The Initial Configuration Wizard of Kaspersky Endpoint Security starts at the end of the application setup procedure. The Initial Configuration Wizard lets you activate the application and gather information about the applications that are included in the operating system. These applications are added to the list of trusted applications whose actions within the operating system are not subject to any restrictions.

The interface of the Initial Configuration Wizard consists of a sequence of pages (steps). You can navigate between the Initial Configuration Wizard pages by using the **Back** and **Next** buttons. To complete the Initial Configuration Wizard procedure, click the **Finish** button. To stop the Initial Configuration Wizard procedure at any stage, click **Cancel**.

If the Initial Configuration Wizard is interrupted for some reason, the already specified settings are not saved. When you start using the application the next time, the Initial Configuration Wizard starts again, and you need to configure the settings again.

IN THIS SECTION:

Completing the update to Kaspersky Endpoint Security 8 for Windows	31
Activating the application.....	31
Activating online	32
Activating by using a key file	32
Completing activation	32
Analyzing the operating system	32
Finishing the Initial Configuration Wizard	33

COMPLETING THE UPDATE TO KASPERSKY ENDPOINT SECURITY 8 FOR WINDOWS

This step is available if you are upgrading a previous version of the application (see the section "About ways to upgrade an old application version" on page [33](#)) to Kaspersky Endpoint Security 8 for Windows.

At this step, you are offered to restart your computer. To complete the update of the previous version of the application and proceed to the initial setup of Kaspersky Endpoint Security 8 for Windows, click the **Finish** button.

ACTIVATING THE APPLICATION

Activating the application requires an Internet connection.

During this step, you can select one of the following Kaspersky Endpoint Security activation options:

- **Activate by using activation code.** To activate the application by using an activation code, select this option and enter the activation code (see the section "About activation code" on page [39](#)).
- **Activate by using a key file.** To activate the application by using a key file, select this option.
- **Activate trial version.** To activate the trial version of the application, select this option. You will be able to use the fully-functional version of the application for the duration of the term that is limited by the license for the trial version of the application. After the license expires, the application functionality is blocked and you cannot activate the trial version again.
- **Activate later.** Select this option if you want to skip the stage of Kaspersky Endpoint Security activation. The user will be able to work with the File Anti-Virus and Firewall components only. The user will be able to update anti-virus databases and modules of Kaspersky Endpoint Security only once after installation. The **Activate later** option is available only at the first start of the Initial Configuration Wizard, immediately after installing the application.

To proceed with the Initial Configuration Wizard, select an activation option and click the **Next** button. To stop the Initial Configuration Wizard, click the **Cancel** button.

ONLINE ACTIVATION

This step is available only when you activate the application by using an activation code. This step is skipped when you activate the trial version of the application or when you activate the application by using a key file.

During this step, Kaspersky Endpoint Security sends data to the activation server to verify the entered activation code:

- If the activation code verification is successful, the Initial Configuration Wizard receives a key file that is installed automatically. The Initial Configuration Wizard then proceeds to the next window.
- If the activation code verification fails, a corresponding message appears. In this case, you are advised to seek advice from the software vendor that sold your license to Kaspersky Endpoint Security.
- If the number of activations with the activation code is exceeded, a corresponding notification appears. The Initial Configuration Wizard is interrupted, and the application suggests that you contact Kaspersky Lab Technical Support.

To return to the previous step of the Initial Configuration Wizard, click the **Back** button. To stop the Initial Configuration Wizard, click the **Cancel** button.

ACTIVATING BY USING A KEY FILE

This step is available only when you activate the commercial version of the application by using a key file.

During this step, you must specify the key file. To do so, click the **View** button and select a file with the .key extension.

After you select a key file, the following license information is displayed in the lower part of the window:

- License number.
- License type and number of computers that are covered by this license
- Application activation date.

License expiration date

To return to the previous step of the Initial Configuration Wizard, click the **Back** button. To proceed with the Initial Configuration Wizard, click the **Next** button. To stop the Initial Configuration Wizard, click the **Cancel** button.

COMPLETING ACTIVATION

During this step, the Initial Configuration Wizard informs you about successful activation of Kaspersky Endpoint Security. License information is also provided:

- License type (commercial or trial) and the number of computers that are covered by the license
- License expiration date

To proceed with the Initial Configuration Wizard, click the **Next** button. To stop the Initial Configuration Wizard, click the **Cancel** button.

ANALYZING THE OPERATING SYSTEM

During this step, information is collected about applications that are included in the operating system. These applications are added to the list of trusted applications whose actions within the operating system are not subject to any restrictions.

Other applications are analyzed after they are started for the first time following Kaspersky Endpoint Security installation.

To stop the Initial Configuration Wizard, click the **Cancel** button.

FINISHING THE INITIAL CONFIGURATION WIZARD

The Initial Configuration Wizard completion window contains information about the completion of the Kaspersky Endpoint Security installation process.

If you want to start Kaspersky Endpoint Security, click the **Finish** button.

If you want to exit the Initial Configuration Wizard without starting Kaspersky Endpoint Security, clear the **Start Kaspersky Endpoint Security 8 for Windows** check box and click **Finish**.

UPGRADING FROM A PREVIOUS VERSION OF THE APPLICATION

This section describes how you can upgrade from a previous version of the application.

IN THIS SECTION:

About ways to upgrade an old application version	33
Upgrading an old application version through the Group Policy Object Editor snap-in	34

ABOUT WAYS TO UPGRADE AN OLD APPLICATION VERSION

You can upgrade the following applications to Kaspersky Endpoint Security 8 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP3
- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Anti-Virus 6.0 for Windows Servers MP3
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4

You can upgrade the old version of the application as follows:

- Locally in interactive mode, by using the Setup Wizard (see the section "Installing the application by using the Setup Wizard" on page [22](#))
- Locally in silent mode, from the command line (see the section "Installing the application from the command line" on page [25](#))
- Remotely, with the help of the Kaspersky Security Center software complex (see the *Kaspersky Security Center Deployment Guide* for details)
- Remotely, by using the Group Policy Object Editor snap-in (see the section "Upgrading an old application version through the Group Policy Object Editor snap-in" on page [34](#))

When updating a previous version of the application to Kaspersky Endpoint Security 8 for Windows, there is no need to remove the previous version of the application. We recommend quitting all active applications before upgrading a previous application version.

When any of the previously listed applications is upgraded to Kaspersky Endpoint Security 8 for Windows, the contents of Quarantine and Backup are not transferred.

UPGRADING AN OLD APPLICATION VERSION THROUGH THE GROUP POLICY OBJECT EDITOR SNAP-IN

The Group Policy Object Editor snap-in lets you update a previous version of Kaspersky Endpoint Security on enterprise workstations that belong to a domain, without using Kaspersky Security Center.

➤ To update a previous version of Kaspersky Endpoint Security through the Group Policy Object Editor snap-in:

1. Create a shared network folder on a computer that acts as domain controller.
2. Place the installation package in MSI format for the new version of Kaspersky Endpoint Security in the shared network folder that you created during the previous step.

In addition, you can copy the setup.ini file to this shared network folder (see the section "Description of setup.ini file settings" on page [27](#)), which contains general Kaspersky Endpoint Security setup settings, along with the install.cfg configuration file and the key file.

3. Open the Group Policy Object Editor snap-in through the MMC console (see the *Microsoft Windows Server help files* for detailed instructions on using the Editor).
4. Create a new installation package of the Group Policy Object Editor snap-in. To do so:
 - a. In the console tree, select **Group Policy Object** → **Computer Configuration** → **Software Settings** → **Software installation**.
 - b. Right-click to bring up the context menu of the **Software installation** node.
 - c. In the context menu, select **New** → **Packet**.
The standard **Open** window of Microsoft Windows Server opens.
 - d. In the standard **Open** window of Microsoft Windows Server, specify the path to the MSI installation package of the new version of Kaspersky Endpoint Security.
 - e. In the **Deploy Software** window, select **Assigned**.
 - f. Click **OK**.
5. In the list of installation packages of the Group Policy Object Editor snap-in, select the installation package that was created during the previous step.
6. Right-click to bring up the context menu of the Group Policy Object Editor snap-in installation package.
7. In the context menu, select **Properties**.
The properties window of the installation package of the Group Policy Object Editor snap-in opens.
8. In the properties window of the installation package of the Group Policy Object Editor snap-in, select the **Update** tab.

9. On the **Updates** tab, add the installation package of the Group Policy Object Editor snap-in that contains the distribution file for the previous version of Kaspersky Endpoint Security.
10. To install the updated version of Kaspersky Endpoint Security while preserving the settings of the previous version, select the option to write over the existing installation package of the Group Policy Object Editor snap-in.

The group policy is enforced on each workstation the next time that the computer is registered in the domain. As a result, the application version is updated on all computers within the domain.

REMOVING THE APPLICATION

This section describes how you can remove Kaspersky Endpoint Security from your computer.

IN THIS SECTION:

About ways to remove the application.....	35
Removing the application by using the Setup Wizard	35
Removing the application from the command line.....	37
Removing the application through the Group Policy Object Editor snap-in	37

ABOUT WAYS TO REMOVE THE APPLICATION

Removing Kaspersky Endpoint Security 8 for Windows leaves the computer and user data unprotected against threats.

There are several ways to remove Kaspersky Endpoint Security 8 for Windows from a computer:

- Locally in interactive mode, by using the Setup Wizard (see the section "Removing the application by using the Setup Wizard" on page [35](#));
- Locally in non-interactive mode, from the command line
- Remotely, with the help of the Kaspersky Security Center software complex (see the *Kaspersky Security Center Deployment Guide* for details)
- Remotely, by using the Group Policy Object Editor snap-in of Microsoft Windows Server (see the section "Removing the application through the Group Policy Object Editor snap-in" on page [37](#)).

REMOVING THE APPLICATION BY USING THE SETUP WIZARD

➔ To remove Kaspersky Endpoint Security by using the Setup Wizard:

1. In the **Start** menu, select **Programs** → **Kaspersky Endpoint Security 8 for Windows** → **Modify, Repair or Remove**.

The Setup Wizard starts.

2. In the **Modify, Repair or Remove** window of the Setup Wizard, click the **Remove** button.
3. Follow the instructions of the Setup Wizard.

IN THIS SECTION:

Step 1. Saving application data for future use	36
Step 2. Confirming application removal.....	36
Step 3. Removing the application. Completing removal.....	36

STEP 1. SAVING APPLICATION DATA FOR FUTURE USE

During this step, you are offered either to remove the application entirely or to preserve application objects. You can specify which of the data that is used by the application you want to save for future use, during the next installation of the application (such as when upgrading to a newer version of the application).

The option **Remove the application entirely** is selected by default. In this case the application settings, information about the activation of the application, and Backup and Quarantine objects are deleted and are no longer available to the user.

➤ *To save application data for future use:*

1. Select **Save application objects**.
2. Select check boxes next to the data types that you want to save:
 - **Activation data** – data that eliminates the need to activate the application in the future by automatically using the current license, as long as the license does not expire before the next installation.
 - **Backup and Quarantine files** – files that are scanned by the application and placed in Backup or Quarantine.

Backup and Quarantine files that are saved after removal of the application can be accessed only from the same version of the application that was used to save the files.

If you plan to use Backup and Quarantine files after application removal, you must restore the files from their storages before removing the application. However, Kaspersky Lab experts do not recommend restoring files from Backup and Quarantine, because this may harm the computer.

- **Operating settings of the application** – application settings values that are selected during configuration.

To proceed with the Setup Wizard, click the **Next** button. To stop the Setup Wizard, click the **Cancel** button.

STEP 2. CONFIRMING APPLICATION REMOVAL

Because removing the application jeopardizes the security of your computer, you are asked to confirm that you want to remove the application. To do so, click the **Remove** button.

To stop removal of the application at any time, you can cancel this operation by clicking the **Cancel** button.

STEP 3. REMOVING THE APPLICATION. COMPLETING REMOVAL

During this step, the Setup Wizard removes the application from the computer. Wait until application removal is complete.

When removing the application, your operating system may require a restart. If you decide to not restart immediately, completion of the application removal procedure is postponed until the operating system is restarted, or until the computer is turned off and then turned on again.

REMOVING THE APPLICATION FROM THE COMMAND LINE

➔ To remove the application from the command line, do one of the following:

- In the command line type the following string: `setup.exe /x`, or

`msiexec.exe /x {D72DD679-A3EC-4FCF-AFAF-12E2552450B6}` to remove the application in interactive mode.

The Setup Wizard starts. Follow the instructions of the Setup Wizard (see the section "Removing the application by using the Setup Wizard" on page [35](#)).

- In the command line, type `setup.exe /s /x` or

`msiexec.exe /x {D72DD679-A3EC-4FCF-AFAF-12E2552450B6} /qn` to remove the application in non-interactive mode (without starting the Setup Wizard).

REMOVING THE APPLICATION THROUGH THE GROUP POLICY OBJECT EDITOR SNAP-IN

➔ To remove Kaspersky Endpoint Security through the Group Policy Object Editor snap-in:

1. Open the Group Policy Object Editor snap-in through the MMC console (see the *Microsoft Windows Server help files* for detailed instructions on using the Editor).
2. In the console tree, select **Group Policy Object** → **Computer Configuration** → **Software Settings** → **Software installation**.
3. In the list of installation packages, select Kaspersky Endpoint Security 8 for Windows.
4. Right-click to bring up the context menu of the installation package and select **All tasks** → **Remove**.
The **Remove Software** window opens.
5. In the **Remove Software** window, select the setting **Immediately remove this application from the computers of all users**.

The group policy is enforced on each workstation the next time that the computer is registered in the domain. As a result, the application is removed on all computers within the domain.

APPLICATION LICENSING

This section contains information about the basic concepts of application activation. This section describes the purpose of the End User License Agreement, the types of licenses, the ways to activate the application, and renew your license.

IN THIS SECTION:

About the End User License Agreement	38
About data submission	38
About the License	39
About activation code	39
About the key file	40
About application activation methods	41
Managing the license	41

ABOUT THE END USER LICENSE AGREEMENT

The End User License Agreement is a binding agreement between you and Kaspersky Lab ZAO, stipulating the terms on which you may use the application.

We recommend carefully reviewing the terms of the End User License Agreement before using the application.

You can review the terms of the End User License Agreement in the following ways:

- When installing a Kaspersky Lab application in interactive mode (see the section "About ways to install the application" on page [21](#)).
- By reading the license.txt file. The document is included in the application distribution kit (see the section "Distribution kit" on page [16](#)).

You are deemed to have accepted the terms of the License Agreement after confirming your agreement to the License Agreement when installing the application.

If you do not accept the terms of the End User License Agreement, you must abort the installation.

ABOUT DATA SUBMISSION

By accepting the End User License Agreement, you agree to automatically submit the checksum data (MD5) of processed files and information that is used in determining website reputations. This information does not contain any personal data or other confidential information. Kaspersky Lab protects the information that is received in accordance with requirements as established by law. You may visit the website <http://support.kaspersky.com> for more details.

ABOUT THE LICENSE

A *license* is a time-limited right to use the application, granted under the End User License Agreement. A license contains a unique activation code for your copy of Kaspersky Endpoint Security.

A valid license entitles you to the following kinds of services:

- The right to use the application on one or several devices.

The number of devices on which you may use the application is specified in the End User License Agreement.

- Assistance from Kaspersky Lab Technical Support.
- The benefits of the complete set of services that Kaspersky Lab or its partners provide during the license validity term (see the section "Service for registered users" on page [19](#)).

The scope of services and application usage term depend on the type of license that is used to activate the application.

The following license types are provided:

- *Trial* – A free license effective for a limited term and intended for trying out the application.

When the trial license expires, all Kaspersky Endpoint Security features become disabled. To continue using the application, you need to buy a commercial license.

- *Commercial* is a paid license that is valid for a limited term and provided when you buy the application.

Application functionality that is available under commercial license depends on the type of commercial license specified in the license certificate:

- *Core / Kaspersky Workspace Security*. Licenses of those types allow the use of protection components on workstations, do not allow the use of control components and application use on file servers and for mobile security and management.
- *Select / Advanced / Total / Kaspersky Business Space Security / Kaspersky Enterprise Space Security / Kaspersky Total Space Security*. Licenses of those types allow the use of all application components on workstations, on file servers, and on mobile devices.

When the commercial license expires, the application continues to work in limited functionality mode. You can still scan the computer for viruses and use other application components, but only with databases that are installed before the expiration of the license. To continue using Kaspersky Endpoint Security in fully functional mode, you must extend your commercial license.

We recommend renewing the license before the expiration of the current license to ensure that your computer stays fully protected.

ABOUT ACTIVATION CODE

An *activation code* is a code that you receive when buying a commercial license for Kaspersky Endpoint Security. You need this code to obtain the key file and to activate the application by installing the key file.

The activation code is a sequence of twenty digits and Latin letters in the format xxxxx-xxxxx-xxxxx-xxxxx.

The license period countdown starts from the moment when you activate the application. When you buy a Kaspersky Endpoint Security license that covers several computers, the license period countdown starts from the moment when you activate the application on the first computer.

If you lose or accidentally delete the activation code after activation, send a request to Kaspersky Lab Technical Support from Personal Cabinet to restore the code (see the section "Obtaining technical support via Personal Cabinet" on page [243](#)).

ABOUT THE KEY FILE

A *key file* is a file of the form xxxxxxxx.key, which enables the user to use Kaspersky Lab applications on the terms of a trial or commercial license. Kaspersky Lab provides a key file based on the activation code when the application is activated by using an activation code, or when Kaspersky Endpoint Security is purchased. You may use the application only when you have a key file.

If the key file is accidentally deleted, you can restore it in one of the following ways:

- Send a request to Technical Support (see the section "Contacting Technical Support" on page [240](#)).
- Obtain a key file on the website (<https://activation.kaspersky.com>) based on your existing activation code.

A *trial key file* is a key file that enables users to try out the application for a limited period of time. A trial key file gives you the right to use the application starting on the day that the application is activated. Kaspersky Lab provides trial key files free of charge upon activation of a trial version of the application.

A *commercial key file* is a key file that contains data that is needed to use the application on the terms of a commercial license. A commercial key file gives you the right to use the application starting on the day that the application is activated. Kaspersky Lab provides a commercial key file based on the activation code that is obtained when buying the application.

A key file contains the following license data:

- License number – a unique number that is needed for a number of purposes, such as to receive technical support from Kaspersky Lab.
- Limit on number of computers – the maximum number of computers on which the application can be activated with the given key file.
- Key file validity term – a specific amount of time that begins at the moment of key file creation. It is determined by the application, depending on the validity term of the license (see the section "About the license" on page [39](#)).
- Key file creation date – the date of creation of the key file that is based on the activation code, marking the start of the countdown of the key file validity term.
- License storage term – a set term that begins at the moment of license creation by Kaspersky Lab specialists. The license storage term may last several years. The application may be activated only before the expiration of this term.
- expiration date of the key file validity term – a date after which the key file cannot be used to activate the application. The expiration date of the key file validity term is calculated from the date when the key file is used for the first time plus the key file validity term, but may not come later than the expiration of the license storage term.

When the expiration date of the key file validity term comes before the expiration of the license storage term, the license storage term is limited by the expiration date of the key file validity term.

- Technical support information.

ABOUT APPLICATION ACTIVATION METHODS

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

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

- When installing the application, by using the Initial Configuration Wizard (see the section "Initial configuration of the application" on page [30](#)).
- Locally from the application interface, by using the Activation Wizard (see the section "Activation Wizard" on page [42](#))
- Remotely, by using the Kaspersky Security Center software complex by creating the key file installation task (see the section "Managing tasks" on page [228](#))
- Remotely by automatically distributing licenses that are stored in the license storage on Administration Server of Kaspersky Security Center to client computers (see the *Kaspersky Security Center Administrator Guide* for details).

MANAGING THE LICENSE

This section describes the available application licensing options.

IN THIS SECTION:

Using the Activation Wizard to activate the application	41
Buying a license	42
Renewing a license	42
Viewing license information	42
Activation Wizard	42

USING THE ACTIVATION WIZARD TO ACTIVATE THE APPLICATION

◆ *To activate Kaspersky Endpoint Security by using the Activation Wizard:*

1. Do one of the following:
 - In the Kaspersky Endpoint Security notice window that appears in the taskbar notification area, click the **Please activate the application** link.
 - In the lower part of the main application window, click the **License** link. In the **License management** window that opens, click the **Activate the application with a new license** button.

The Activation Wizard (on page [42](#)) starts.

2. Follow the instructions of the Activation Wizard.

BUYING A LICENSE

You may buy a license after installing the application. After buying a license, you receive an activation code or key file with which you must activate the application (see the section "Using the Activation Wizard to activate the application" on page [41](#)).

➤ *To purchase a license:*

1. Open the main application window (on page [46](#)).
2. In the lower part of the main application window, click the **License** link to open the **License management** window.
3. Do one of the following in the **License management** window:
 - Click the **Buy license** button if no license has been installed or you have a trial license.
 - If you have a commercial license installed, click the **Renew license** button.

A window will open with the website of the Kaspersky Lab online store, where you can buy a license.

RENEWING A LICENSE

When your license approaches expiration, you can renew it. This ensures that your computer remains protected after expiration of the existing license and before you activate the application with a new license.

➤ *To renew a license:*

1. Purchase (see the section "Buying a license" on page [42](#)) a new activation code or key file.
2. Activate the application (see the section "Using the Activation Wizard to activate the application" on page [41](#)) by using the activation code or key file that you have purchased.

This causes an additional license to be added, which is applied automatically upon expiration of the current Kaspersky Endpoint Security license.

VIEWING LICENSE INFORMATION

➤ *To view license information:*

1. Open the main application window (on page [46](#)).
2. In the lower part of the main application window, click the **License** link.

The **License management** window opens. License information is displayed in the section that is located in the upper part of the **License management** window.

ACTIVATION WIZARD

The interface of the Activation Wizard consists of a sequence of pages (steps). You can navigate between Activation Wizard pages by using the **Back** and **Next** buttons. To exit the Activation Wizard, click the **Finish** button. To stop the Activation Wizard at any stage, click the **Cancel** button.

IN THIS SECTION:

Activating the application.....	43
Activating online.....	43
Activating by using a key file.....	43
Completing activation.....	44

ACTIVATING THE APPLICATION

Activating the application requires an Internet connection.

During this step, you can select one of the following Kaspersky Endpoint Security activation options:

- **Activate by using activation code.** To activate the application by using an activation code, select this option and enter the activation code (see the section "About activation code" on page [39](#)).
- **Activate by using a key file.** To activate the application by using a key file, select this option.
- **Activate trial version.** To activate the trial version of the application, select this option. You will be able to use the fully-functional version of the application for the duration of the term that is limited by the license for the trial version of the application. After the license expires, the application functionality is blocked and you cannot activate the trial version again.

To proceed with the Activation Wizard, select an application activation option and click **Next**. To stop the Activation Wizard, click the **Cancel** button.

ACTIVATING ONLINE

This step is available only when you activate the application by using an activation code. This step is skipped when you activate the trial version of the application or when you activate the application by using a key file.

During this step, Kaspersky Endpoint Security sends data to the activation server to verify the entered activation code:

- If the activation code is successfully verified, the Activation Wizard receives a key file. The key file is installed automatically. The Activation Wizard automatically proceeds to the following step.
- If the activation code verification fails, a corresponding message appears. In this case, you are advised to seek advice from the software vendor that sold your license to Kaspersky Endpoint Security.
- If the number of activations with the activation code is exceeded, a corresponding notification appears. The Activation Wizard is interrupted, and the application suggests that you contact Kaspersky Lab Technical Support.

To return to the previous step of the Activation Wizard, click the **Back** button. To stop the Activation Wizard, click the **Cancel** button.

ACTIVATING BY USING A KEY FILE

This step is available only when you activate the commercial version of the application by using a key file.

During this step, you must specify the key file. To do so, click the **View** button and select a file with the .key extension.

After you select a key file, the following license information is displayed in the lower part of the window:

- License number.
- License type and number of computers that are covered by this license
- Application activation date.
- License expiration date

To return to the previous step of the Activation Wizard, click the **Back** button. To proceed with the Activation Wizard, click the **Next** button. To stop the Activation Wizard, click the **Cancel** button.

COMPLETING ACTIVATION

During this step, the Activation Wizard informs you about successful activation of Kaspersky Endpoint Security. License information is also provided:

- License type (commercial or trial) and the number of computers that are covered by the license
- License expiration date

To exit the Activation Wizard, click the **Finish** button.

APPLICATION INTERFACE

This section describes the basic elements of the graphical interface of the application: the application icon and its context menu, main application window, and application settings window.

IN THIS SECTION:

Application icon in the taskbar notification area	45
Application icon context menu.....	46
Main application window	46
Application settings window	48

APPLICATION ICON IN THE TASKBAR NOTIFICATION AREA







Immediately after installation of Kaspersky Endpoint Security, the application icon appears in the Microsoft Windows taskbar notification area.

The icon serves the following purposes:

- It indicates application activity.
- It acts as a shortcut to the context menu and main window of the application.

Indication of application activity

The application icon serves as an indicator of application activity. It reflects the status of computer protection and shows the operations that the application is currently performing:

- The  icon signifies that all protection components of the application are enabled.
- The  icon signifies that Kaspersky Endpoint Security is scanning an email message.
- The  icon signifies that Kaspersky Endpoint Security is scanning incoming and outgoing network traffic.
- The  icon signifies that Kaspersky Endpoint Security is updating application databases and modules.
- The  icon signifies that important events that require your attention have occurred in the operation of Kaspersky Endpoint Security. For example, File Anti-Virus is disabled or the application databases are out of date.
- The  icon signifies that critical events have occurred in the operation of Kaspersky Endpoint Security. For example, a failure in the operation of one or more components, or corruption of the application databases.

The icon is animated by default: for example, when Kaspersky Endpoint Security scans an email message, a small envelope symbol pulsates against the background of the application icon; when Kaspersky Endpoint Security updates its databases and modules, a globe symbol revolves against the background of the application icon.

APPLICATION ICON CONTEXT MENU

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

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

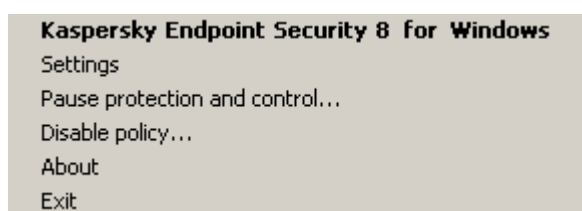


Figure 1. Application icon context menu

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.

MAIN APPLICATION WINDOW

The main window of Kaspersky Endpoint Security contains interface elements that provide access to the main functions of the application.

The main window is divided into three parts (see the following image):

- Located in the upper part of the window are interface elements that let you view the following information:
 - Application details
 - Reputation database statistics
 - List of unprocessed files
 - List of detected vulnerabilities
 - List of quarantined files
 - Backup storage of copies of infected files that the application has deleted
 - Reports on events that have occurred during operation of the application in general or its separate components, or during the performance of tasks

- The **Protection and Control** tab allows you to adjust the operation of application components and tasks. The **Protection and Control** tab is displayed when you open the main application window.
- The **Settings** tab allows you to edit the default application settings.

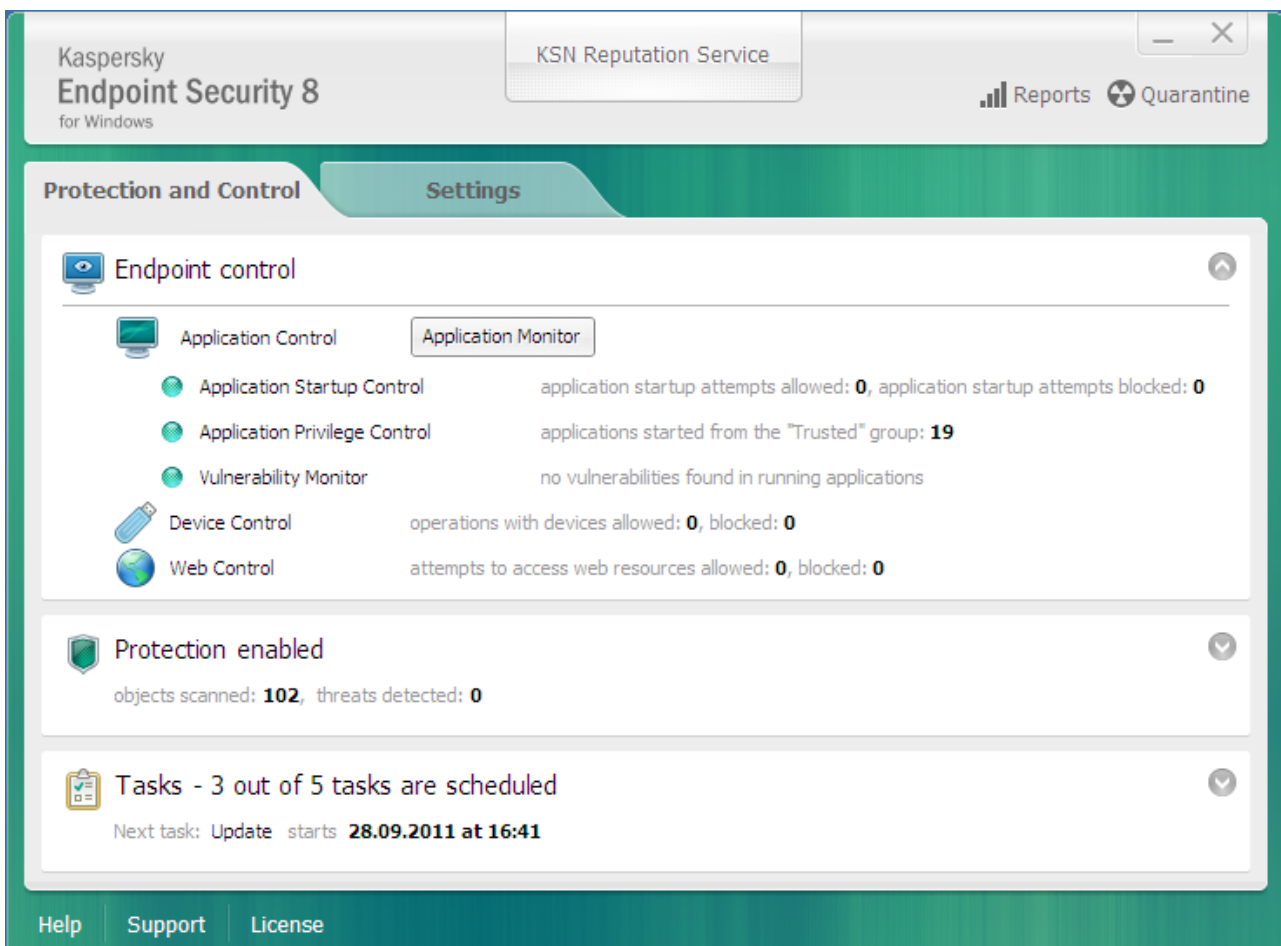


Figure 2. Main application window

You can use the following links:

- **Help.** Clicking this link takes you to the help system of Kaspersky Endpoint Security.
- **Support.** Clicking this link opens the **Support** window, which contains information on the operating system, the current version of Kaspersky Endpoint Security, and links to Kaspersky Lab information resources.
- **License.** Clicking this link opens the **License management** window, which contains the details of the currently active license.

You can open the main window of Kaspersky Endpoint Security in one of the following ways:

- Rest the mouse pointer over the application icon in the taskbar notification area of Microsoft Windows and click.
- Select **Kaspersky Endpoint Security** from the application icon context menu (see the section "Application icon context menu" on page [46](#)).

APPLICATION SETTINGS WINDOW

The Kaspersky Endpoint Security settings window lets you configure overall application settings, individual components, reports and storages, scan tasks, update tasks, vulnerability scan tasks, and interaction with Kaspersky Security Network.

- The application settings window consists of two parts (see the following figure).
- The left part of the window contains application components, tasks, and other configurable items.
- The right part of the window contains controls that you can use to configure the item that is selected in the left part of the window.

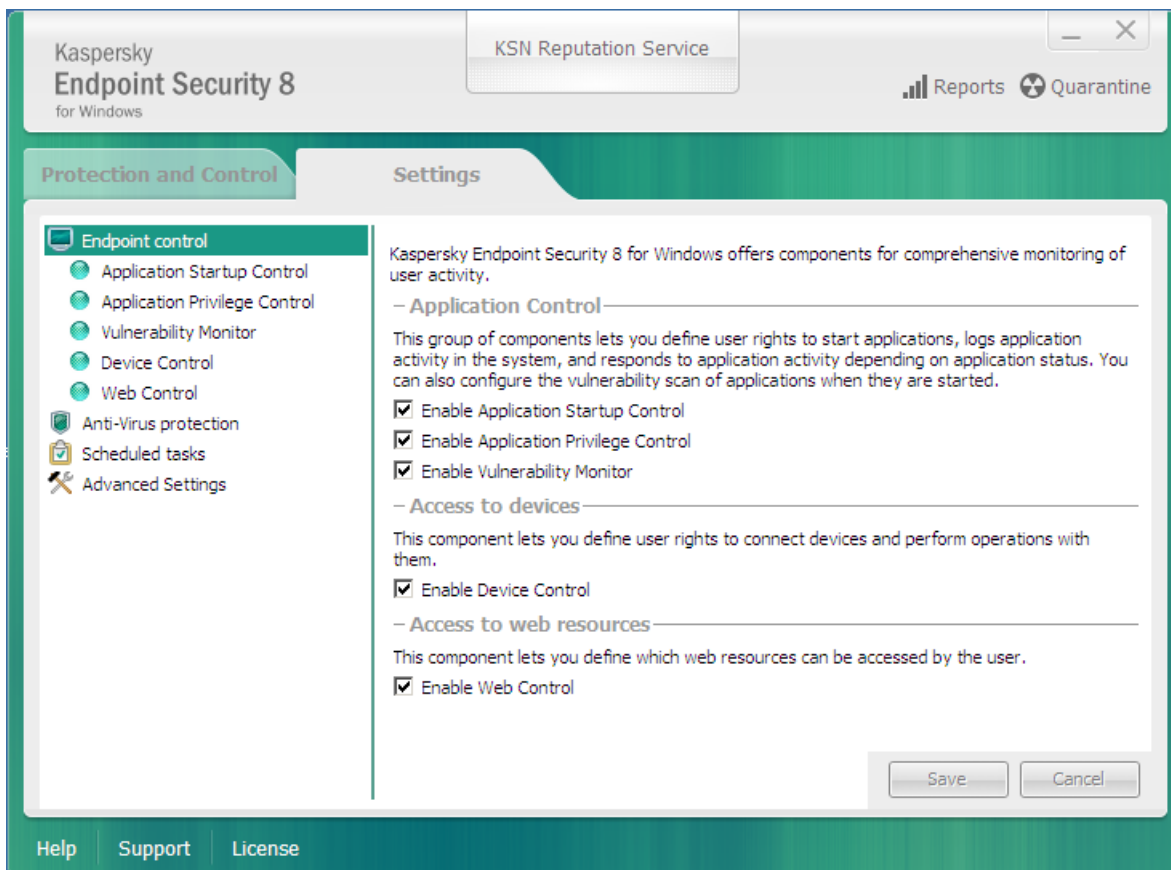


Figure 3. Application settings window

As in the main window, you can use the following links:

- **Help.** Clicking this link takes you to the help system of Kaspersky Endpoint Security.
- **Support.** Clicking this link opens the **Support** window, which contains information on the operating system, the current version of Kaspersky Endpoint Security, and links to Kaspersky Lab information resources.
- **License.** Clicking this link opens the **License management** window, which contains the details of the currently active license.

You can open the application settings window in one of the following ways:

- Select the **Settings** tab in the main application window (see the section "Main application window" on page [46](#)).
- Select **Settings** from the application context menu (see the section "Application icon context menu" on page [46](#)).

STARTING AND STOPPING THE APPLICATION

This section describes how you can configure automatic startup of the application, start or stop the application manually, and pause or resume protection and control components.

IN THIS SECTION:

Enabling and disabling automatic startup of the application.....	49
Starting and stopping the application manually.....	49
Pausing and resuming computer protection and control.....	50

ENABLING AND DISABLING AUTOMATIC STARTUP OF THE APPLICATION

Automatic startup means that Kaspersky Endpoint Security starts immediately after operating system startup, without user intervention. This application startup option is enabled by default.

After installation, Kaspersky Endpoint Security starts automatically for the first time. Subsequently the application starts automatically after operating system startup.

➤ *To enable or disable automatic startup of the application:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.

The anti-virus protection settings are shown in the right part of the window.
3. Do one of the following:
 - To enable automatic application startup, select the **Start Kaspersky Endpoint Security on computer startup** check box.
 - To disable automatic application startup, clear the **Start Kaspersky Endpoint Security on computer startup** check box.
4. To save changes, click the **Save** button.

STARTING AND STOPPING THE APPLICATION MANUALLY

Kaspersky Lab specialists do not recommend stopping Kaspersky Endpoint Security manually, because doing so exposes the computer and your personal data to threats. If necessary, you can pause computer protection (see the section "Pausing and resuming computer protection and control" on page [50](#)) for as long as you need to, without stopping the application.

Kaspersky Endpoint Security needs to be started manually if you have previously disabled automatic startup of the application (see the section "Enabling and disabling automatic startup of the application" on page [49](#)).

➤ *To start the application manually,*

in the **Start** menu, select **Programs** → **Kaspersky Endpoint Security 8 for Windows**.



➤ *To stop the application manually:*

1. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
2. In the context menu, select **Exit**.

PAUSING AND RESUMING COMPUTER PROTECTION AND CONTROL

Pausing computer protection and control means disabling all protection and control components of Kaspersky Endpoint Security for a time.

The application status is indicated by the application icon in the taskbar notification area (see the section "Application icon in the taskbar notification area" on page [45](#)).

- The  icon signifies that computer protection and control are paused.
- The  icon signifies that computer protection and control have been resumed.

Pausing or resuming computer protection and control does not affect scan or update tasks.

If any network connections are already established when you pause or resume computer protection and control, a notification about the termination of these network connections is displayed.

➤ *To pause or resume computer protection and control:*

1. To pause computer protection and control:
 - a. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
 - b. In the context menu, select **Pause protection and control**.

The **Pause protection and control** window opens.
 - c. Select one of the following options:
 - **Pause for the specified time** – Computer protection and control resume after the amount of time that is specified in the drop-down list below has elapsed. You can select the necessary amount of time in the drop-down list.
 - **Pause until restart** – Computer protection and control resume after you quit and reopen the application or restart the operating system. Automatic startup of the application must be enabled to use this option.
 - **Pause** – Computer protection and control resume when you decide to re-enable them.
2. If you decide to resume computer protection and control, you can do so at any time, regardless of the protection and control pause option that you selected previously. To resume computer protection and control:
 - a. Right-click to bring up the context menu of the application icon that is in the taskbar notification area.
 - b. In the context menu, select **Resume protection and control**.

PROTECTING THE COMPUTER FILE SYSTEM. FILE ANTI-VIRUS

This section contains information about File Anti-Virus and instructions on how to configure the component settings.

IN THIS SECTION:

About File Anti-Virus	51
Enabling and disabling File Anti-Virus.....	51
Automatically pausing File Anti-Virus	52
Configuring File Anti-Virus.....	53

ABOUT FILE ANTI-VIRUS

File Anti-Virus prevents infection of the computer's file system. By default, File Anti-Virus starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started on your computer and on all drives that are attached to it for the presence of viruses and other malware.

File Anti-Virus uses the signature and heuristic analysis methods and the iChecker and iSwift technologies.

When the user or an application attempts to access a protected file, File Anti-Virus checks whether the iChecker and iSwift databases contain information about this file, and uses this information to decide whether it is necessary to scan the file.

If Kaspersky Endpoint Security detects a threat in the file, it assigns one of the following statuses to this file:

- A status that indicates the type of malicious program that is detected (for example, *virus* or *Trojan*).
- *Potentially infected* status, if the scan cannot determine whether or not the file is infected. The file may contain a code sequence that is typical of viruses and other malware, or modified code from a known virus.

The application then displays a notification (see page [199](#)) of the threat detected within the file and takes the action on the file that is specified in the settings of File Anti-Virus (see the section "Changing the action to take on infected files" on page [55](#)).

ENABLING AND DISABLING FILE ANTI-VIRUS

By default, File Anti-Virus is enabled, running in the mode that is recommended by Kaspersky Lab's experts. You can disable File Anti-Virus, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➤ *To enable or disable File Anti-Virus on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.



The **Protection** section opens.

4. Right-click to bring up the context menu of the line with information about the File Anti-Virus component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable File Anti-Virus, select **Enable** in the menu.

The component status icon , which is displayed on the left in the **File Anti-Virus** line, changes to the icon .

- To disable File Anti-Virus, select **Disable** in the menu.

The component status icon , which is displayed on the left in the **File Anti-Virus** line, changes to the icon .

➤ *To enable or disable File Anti-Virus from the application settings window:*

1. Open the application settings window.
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.

In the right part of the window, the settings of the File Anti-Virus component are displayed.

3. Do one of the following:

- If you want to enable File Anti-Virus, select the **Enable File Anti-Virus** check box.
- If you want to disable File Anti-Virus, clear the **Enable File Anti-Virus** check box.

4. To save changes, click the **Save** button.

AUTOMATICALLY PAUSING FILE ANTI-VIRUS

You can configure the component to automatically pause at a specified time or when handling specified programs.

Pausing File Anti-Virus when it conflicts with some programs is an emergency measure. In case of any conflicts during the operation of a component, we recommend contacting Kaspersky Lab Technical Support (<http://support.kaspersky.com/helpdesk.html>). The support specialists will help you to set up Kaspersky Endpoint Security to run simultaneously with other programs on your computer.

➤ *To configure automatic pausing of File Anti-Virus:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.

In the right part of the window, the settings of the File Anti-Virus component are displayed.

3. In the **Security level** section, click the **Settings** button.

The **File Anti-Virus** window opens.

4. In the **File Anti-Virus** window, select the **Additional** tab.

5. In the **Pause task** section:

- To configure automatic pausing of File Anti-Virus at a specified time, select the **By schedule** check box and click the **Schedule** button.

The **Pause task** window opens.

- To configure automatic pausing of File Anti-Virus at startup of specified applications, select the **At application startup** check box and click the **Select** button.

The **Applications** window opens.

6. Do one of the following:

- If you are configuring automatic pausing of File Anti-Virus at a specified time, in the **Pause task** window, use the **Pause task at** and **Resume task at** fields to specify the time period (in HH:MM format) during which File Anti-Virus is to be paused. Then click **OK**.
- If you are configuring automatic pausing of File Anti-Virus at startup of specified applications, use the **Add**, **Edit**, and **Delete** buttons in the **Applications** window to create a list of applications during whose operation File Anti-Virus is to be paused. Then click **OK**.

7. In the **File Anti-Virus** window, click **OK**.

8. To save changes, click the **Save** button.

CONFIGURING FILE ANTI-VIRUS

You can do the following to configure File Anti-Virus:

- Change the file security level.

You can select one of the preset file security levels or configure security level settings on your own. If you have changed the file security level settings, you can always revert to the recommended file security level settings.

- Change the action that is performed by File Anti-Virus on detection of an infected file.
- Edit the protection scope of File Anti-Virus.

You can expand or restrict the protection scope by adding or removing scan objects, or by changing the type of files to be scanned.

- Configure Heuristic Analyzer.

File Anti-Virus uses a technique that is called signature analysis. During signature analysis, File Anti-Virus matches the detected object with records in its databases. Following the recommendations of Kaspersky Lab's experts, signature analysis is always enabled.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, File Anti-Virus analyzes the activity of objects in the operating system. Heuristic analysis allows detecting new malicious objects for which no records are currently available in the databases.

- Select the scan technologies.

You can enable the use of the iChecker and iSwift technologies, which optimize the speed of file scanning by excluding files that have not been modified since the most recent scan.

- Optimize scanning.

You can optimize the file scanning that is performed by File Anti-Virus, reducing the scan time and increasing the operating speed of Kaspersky Endpoint Security. This can be achieved by scanning only new files and those files that have been modified since the previous scan. This mode applies both to simple and to compound files.

- Configure scanning of compound files.
- Change the file scan mode.

IN THIS SECTION:

Changing the file security level.....	54
Changing the action to take on infected files.....	55
Editing the protection scope of File Anti-Virus.....	55
Using Heuristic Analyzer with File Anti-Virus.....	56
Using scan technologies in the operation of File Anti-Virus.....	57
Optimizing file scanning	58
Scanning compound files	58
Changing the scan mode	59

CHANGING THE FILE SECURITY LEVEL

To protect the computer's file system, File Anti-Virus applies various groups of settings. These groups of settings are called *file security levels*. There are three pre-installed file security levels: **High**, **Recommended**, and **Low**. The **Recommended** file security level is considered the optimal group of settings, and is recommended by Kaspersky Lab.

➤ *To change the file security level:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.

In the right part of the window, the settings of the File Anti-Virus component are displayed.
3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed file security levels (**High**, **Recommended**, or **Low**), use the slider to select one.

- If you want to configure a custom file security level, click the **Settings** button and, in the **File Anti-Virus** window that opens, enter settings.

After you configure a custom file security level, the name of the file security level in the **Security level** section changes to **Custom**.

- If you want to change the file security level to **Recommended**, click the **Default** button.
4. To save changes, click the **Save** button.

CHANGING THE ACTION TO TAKE ON INFECTED FILES

➤ *To change the action to take on infected files:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.
In the right part of the window, the settings of the File Anti-Virus component are displayed.
3. In the **Action on threat detection** section, select the required option:
 - **Select action automatically.**
 - **Perform action: Disinfect. Delete if disinfection fails.**
 - **Perform action: Disinfect.**
 - **Perform action: Delete.**
 - **Perform action: Block.**
4. To save changes, click the **Save** button.

EDITING THE PROTECTION SCOPE OF FILE ANTI-VIRUS

The protection scope refers to the objects that the component scans when enabled. The protection scopes of different components have different properties. The location and type of files to be scanned are properties of the protection scope of File Anti-Virus. By default, File Anti-Virus scans only infectable files that are stored on hard drives, network drives, or removable media.

➤ *To create the protection scope:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.
In the right part of the window, the settings of the File Anti-Virus component are displayed.
3. In the **Security level** section, click the **Settings** button.
The **File Anti-Virus** window opens.
4. In the **File Anti-Virus** window, on the **General** tab, in the **File types** section, specify the type of files that you want to scan with File Anti-Virus:
 - If you want to scan all files, select **All files**.

- If you want to scan files of formats which are the most vulnerable to infection, select **Files scanned by format**.
- If you want to scan files with extensions that are the most vulnerable to infection, select **Files scanned by extension**.

When selecting the type of files to scan, remember the following information:

- There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high.
- An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then regardless of the extension, File Anti-Virus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware.

5. In the **Protection scope** list, do one of the following:

- If you want to add a new object to the list of objects to be scanned, click the **Add** button.
- If you want to change the location of an object, select one from the list of objects to be scanned and click the **Edit** button.

The **Select object to scan** window opens.

- If you want to remove an object from the list of objects to be scanned, select one from the list of objects to be scanned and click the **Remove** button.

A window for confirming deletion opens.

6. Do one of the following:

- If you want to add a new object or change the location of an object from the list of objects to be scanned, select one in the **Select object to scan** window and click the **Add** button.

All objects that are selected in the **Select object to scan** window are displayed in the **File Anti-Virus** window, in the **Protection scope** list.

Then click **OK**.

- If you want to remove an object, click the **Yes** button in the window for confirming removal.

7. If necessary, repeat steps 5–6 for adding, moving, or removing objects from the list of objects to be scanned.

8. To exclude an object from the list of objects to be scanned, clear the check box next to the object in the **Protection scope** list. However, the object remains on the list of objects to be scanned, though it is excluded from scanning by File Anti-Virus.

9. In the **File Anti-Virus** window, click **OK**.

10. To save changes, click the **Save** button.

USING HEURISTIC ANALYZER WITH FILE ANTI-VIRUS

➤ *To configure the use of Heuristic Analyzer in the operation of File Anti-Virus:*

1. Open the application settings window (on page [48](#)).

2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.

In the right part of the window, the settings of the File Anti-Virus component are displayed.

3. In the **Security level** section, click the **Settings** button.

The **File Anti-Virus** window opens.

4. In the **File Anti-Virus** window, select the **Performance** tab.

5. In the **Scan methods** section:

- If you want File Anti-Virus to use heuristic analysis, select the **Heuristic Analysis** check box and use the slider to set the level of heuristic analysis detail: **Light scan**, **Medium scan**, or **Deep scan**.
- If you do not want File Anti-Virus to use heuristic analysis, clear the **Heuristic Analysis** check box.

6. Click **OK**.

7. To save changes, click the **Save** button.

USING SCAN TECHNOLOGIES IN THE OPERATION OF FILE ANTI-VIRUS

➔ *To configure the use of scan technologies in the operation of File Anti-Virus:*

1. Open the application settings window (on page [48](#)).

2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.

In the right part of the window, the settings of the File Anti-Virus component are displayed.

3. In the **Security level** section, click the **Settings** button.

The **File Anti-Virus** window opens.

4. In the **File Anti-Virus** window, select the **Additional** tab.

5. In the **Scan technologies** section:

- Select the check boxes opposite the names of technologies that you want to use in the operation of File Anti-Virus.
- Clear the check boxes opposite the names of technologies that you do not want to use in the operation of File Anti-Virus.

6. Click **OK**.
7. To save changes, click the **Save** button.

OPTIMIZING FILE SCANNING

◆ To optimize file scanning:

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.
In the right part of the window, the settings of the File Anti-Virus component are displayed.
3. Click the **Settings** button.
The **File Anti-Virus** window opens.
4. In the **File Anti-Virus** window, select the **Performance** tab.
5. In the **Scan optimization** section, select the **Scan only new and changed files** check box.
6. Click **OK**.
7. To save changes, click the **Save** button.

SCANNING COMPOUND FILES

A common technique of concealing viruses and other malware is to implant them in compound files, such as archives or databases. To detect viruses and other malware that are hidden in this way, the compound file must be unpacked, which may slow down scanning. You can limit the set of compound files to be scanned, thus speeding up scanning.

◆ To configure scanning of compound files:

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.
In the right part of the window, the settings of the File Anti-Virus component are displayed.
3. In the **Security level** section, click the **Settings** button.
The **File Anti-Virus** window opens.
4. In the **File Anti-Virus** window, select the **Performance** tab.
5. In the **Scanning of compound files** section, specify the types of compound files that you want to scan: archives, installation packages, or embedded OLE objects.
6. If the **Scan only new and changed files** check box is cleared in the **Scan optimization** section, you can specify for each type of compound file whether to scan all files of this type or new ones only. To make your choice, click the **all / new** link next to the name of a type of compound file. This link changes its value after you click it.

If the **Scan only new and changed files** check box is selected, only new files are scanned.
7. Click the **Additional** button.
The **Compound files** window opens.

8. In the **Background scan** section, do one of the following:
 - If you do not want File Anti-Virus to unpack compound files in background mode, clear the **Extract compound files in the background** check box.
 - If you want File Anti-Virus to unpack large-sized compound files in background mode, select the **Extract compound files in the background** check box and specify the required value in the **Minimum file size** field.

9. In the **Size limit** section, do one of the following:
 - If you do not want File Anti-Virus to unpack large-sized compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field.
 - If you want File Anti-Virus to unpack large-sized compound files, clear the **Do not unpack large compound files** check box.

A file is considered large if its size exceeds the value in the **Maximum file size** field.

File Anti-Virus scans large-sized files that are extracted from archives, regardless of whether or not the **Do not unpack large compound files** check box is selected.

10. Click **OK**.
11. In the **File Anti-Virus** window, click **OK**.
12. To save changes, click the **Save** button.

CHANGING THE SCAN MODE

Scan mode means the condition under which File Anti-Virus starts to scan files. By default, Kaspersky Endpoint Security scans files in smart mode. In this file scan mode, File Anti-Virus decides whether or not to scan files after analyzing operations that are performed with the file by the user, by an application on behalf of the user (under the account that was used to log in or a different user account), or by the operating system. For example, when working with a Microsoft Office Word document, Kaspersky Endpoint Security scans the file when it is first opened and last closed. Intermediate operations that overwrite the file do not cause it to be scanned.

➔ *To change the file scan mode:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **File Anti-Virus**.
In the right part of the window, the settings of the File Anti-Virus component are displayed.
3. In the **Security level** section, click the **Settings** button.
The **File Anti-Virus** window opens.
4. In the **File Anti-Virus** window, select the **Additional** tab.

5. In the **Scan mode** section, select the required mode:
 - **Smart mode.**
 - **On access and modification.**
 - **On access.**
 - **On execution.**
6. Click **OK**.
7. To save changes, click the **Save** button.

SYSTEM WATCHER

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

This section contains information about System Watcher and instructions on how to configure the component settings.

IN THIS SECTION:

About System Watcher.....	61
Enabling and disabling System Watcher	61
Using behavior stream signatures (BSS)	63
Rolling back malware actions during disinfection	63

ABOUT SYSTEM WATCHER

System Watcher collects data on the actions of applications on your computer and passes this information to other components for more reliable protection.

Behavior stream signatures

Behavior Stream Signatures (BSS) (also called "behavior stream signatures") contain sequences of application actions that Kaspersky Endpoint Security classifies as dangerous. If application activity matches a behavior stream signature, Kaspersky Endpoint Security performs the specified action. Kaspersky Endpoint Security functionality based on behavior stream signatures provides proactive defense for the computer.

By default, if the activity of an application matches a behavior stream signature, System Watcher moves the executable file of the application to Quarantine (see the section "Managing Quarantine and Backup" on page [202](#)).

Rolling back actions that have been performed by malware

Based on information that System Watcher collects, Kaspersky Endpoint Security can roll back actions that have been performed by malware in the operating system while performing disinfection.

A rollback of malware actions can be initiated by Proactive Defense, File Anti-Virus (see the section "Protecting the computer file system. File Anti-Virus" on page [51](#)), or during a virus scan (see the section "Scan" on page [168](#)).

Rolling back malware operations affects a strictly defined set of data. It causes no negative consequences for the operating system or the integrity of data on your computer.

ENABLING AND DISABLING SYSTEM WATCHER

By default, System Watcher is enabled and runs in the mode that Kaspersky Lab specialists recommend. You can disable System Watcher, if necessary.

It is not recommended to disable System Watcher unnecessarily, because doing so reduces the performance of protection components that may require data from System Watcher to classify potential threats that they detect.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➔ *To enable or disable System Watcher on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.



The **Protection** section opens.

4. Right-click to display the context menu of the line with information about the System Watcher component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable System Watcher, select **Enable**.

The component status icon , which is displayed on the left in the **System Watcher** line, changes to the  icon.

- To disable System Watcher, select **Disable**.

The component status icon , which is displayed on the left in the **System Watcher** line, changes to the  icon.

➔ *To enable or disable System Watcher from the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **System Watcher**.

In the right part of the window, the settings of the **System Watcher** component are displayed.

3. Do one of the following:

- To enable System Watcher, select the **Enable System Watcher** check box
- To disable System Watcher, clear the **Enable System Watcher** check box.

4. To save changes, click the **Save** button.

USING BEHAVIOR STREAM SIGNATURES (BSS)

➤ *To use behavior stream signatures (BSS):*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **System Watcher**.
In the right part of the window, the settings of the **System Watcher** component are displayed.
3. In the **Proactive Defense** section, select the **Use updatable patterns of dangerous activity (BSS)** check box.
4. Select the required action from the **On detecting malware activity** list:
 - **Select action automatically.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security performs the default action that is specified by Kaspersky Lab specialists. By default, Kaspersky Endpoint Security moves the executable file of the malicious application to Quarantine.
 - **Move file to Quarantine.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security moves the executable file of this application to Quarantine.
 - **Terminate the malicious program.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security terminates the relevant application.
 - **Skip.** If this item is selected, on detecting malicious activity Kaspersky Endpoint Security does not take any action on the executable file of this application.
5. To save changes, click the **Save** button.

ROLLING BACK MALWARE ACTIONS DURING DISINFECTION

➤ *To enable or disable the rollback of malware actions during disinfection:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **System Watcher**.
In the right part of the window, the settings of the **System Watcher** component are displayed.
3. Do one of the following:
 - If you want Kaspersky Endpoint Security to roll back actions that were performed by malware in the operating system while performing disinfection, select the **Roll back malware actions during disinfection** check box.
 - If you want Kaspersky Endpoint Security to ignore actions that were performed by malware in the operating system while performing disinfection, clear the **Roll back malware actions during disinfection** check box.
4. To save changes, click the **Save** button.

EMAIL PROTECTION. MAIL ANTI-VIRUS

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).



This section contains information about Mail Anti-Virus and instructions on how to configure the component settings.

IN THIS SECTION:

About Mail Anti-Virus.....	64
Enabling and disabling Mail Anti-Virus	64
Configuring Mail Anti-Virus.....	65

ABOUT MAIL ANTI-VIRUS

Mail Anti-Virus scans incoming and outgoing email messages for viruses and other malware. It starts together with Kaspersky Endpoint Security, continuously remains active in computer memory, and scans all email messages that are sent or received via the POP3, SMTP, IMAP, MAPI, and NNTP protocols.

The Mail Anti-Virus icon in the taskbar notification area indicates that the application is running. The icon appears as  every time that an email message is scanned. 

Mail Anti-Virus intercepts each email message that is received or sent by the user. If no threats are detected in the message, it becomes available to the user.

If a threat is detected in the file, Kaspersky Endpoint Security assigns one of the following statuses to this file:

- A status that indicates the type of malicious program that is detected (for example, *virus* or *Trojan*).
- *Potentially infected* status if the scan cannot determine whether or not the email message is infected. The email message may possibly contain a code sequence that is typical of viruses or other malware, or the modified code of a known virus.

The application then blocks the email message, displays a notification (see page [199](#)) (if this is specified by the notification settings) about the detected threat, and takes the action on the message that is specified in the settings of Mail Anti-Virus (see the section "Changing the action to take on infected email messages" on page [67](#)).

For the Microsoft Office Outlook and The Bat! email clients, extension modules (plug-ins) allow you to fine-tune the mail scanning settings. The Mail Anti-Virus plug-in is embedded in the Microsoft Office Outlook and The Bat! mail programs during installation of Kaspersky Endpoint Security.

Mail Anti-Virus does not support protocols that ensure encrypted data transfer.

ENABLING AND DISABLING MAIL ANTI-VIRUS

By default, Mail Anti-Virus is enabled, running in a mode that is recommended by Kaspersky Lab's experts. You can disable Mail Anti-Virus, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➤ *To enable or disable Mail Anti-Virus on the Protection and Control tab of the main application window:*

1. Open the main application window.

2. Select the **Protection and Control** tab.

3. Click the **Protection** section.



The **Protection** section opens.

4. Right-click to bring up the context menu of the line with information about the Mail Anti-Virus component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable Mail Anti-Virus, select **Enable** in the menu.

The component status icon , which is displayed on the left in the **Mail Anti-Virus** line, changes to the icon .

- To disable Mail Anti-Virus, select **Disable** in the menu.

The component status icon , which is displayed on the left in the **Mail Anti-Virus** line, changes to the icon .

➤ *To enable or disable Mail Anti-Virus from the application settings window:*

1. Open the application settings window.

2. In the left part of the window, in the Anti-Virus protection section, select **Mail Anti-Virus**.

In the right part of the window, the settings of the Mail Anti-Virus component are displayed.

3. Do one of the following:

- If you want to enable Mail Anti-Virus, select the **Enable Mail Anti-Virus** check box.
- If you want to disable Mail Anti-Virus, clear the **Enable Mail Anti-Virus** check box.

4. To save changes, click the **Save** button.

CONFIGURING MAIL ANTI-VIRUS

You can do the following to configure Mail Anti-Virus:

- Change the security level.

You can select one of the pre-installed email security levels or configure a custom email security level.

If you have changed the email security level settings, you can always revert to the recommended email security level settings.

- Change the action that Kaspersky Endpoint Security performs on infected email messages.
- Edit the protection scope of Mail Anti-Virus.
- Configure scanning of compound file attachments in email messages.

You can enable or disable the scanning of archives that are attached to email messages and limit the maximum size of email attachments to be scanned and the maximum attachment scan duration.

- Configure filtering of email attachments by type.

Filtering of email attachments by type allows files of the specified types to be automatically renamed or deleted.

- Configure Heuristic Analyzer.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of applications in the operating system. Heuristic analysis can detect new threats in email messages for which there are currently no records in the Kaspersky Endpoint Security databases.

- Configure email scanning in Microsoft Office Outlook.

A plug-in is designed for Microsoft Office Outlook, which allows comfortably adjusting email scan settings.

- Configure email scanning in The Bat!.

A plug-in is designed for The Bat!, which allows comfortably adjusting email scan settings.

When working with other email clients, including Microsoft Outlook Express®, Windows Mail, and Mozilla™ Thunderbird™, the Mail Anti-Virus component scans emails sent via the SMTP, POP3, IMAP, and NNTP protocols.

When working with Mozilla Thunderbird, Mail Anti-Virus does not scan email messages that are transmitted via the IMAP protocol for viruses and other threats if filters are used to move email messages from the **Inbox** folder.

IN THIS SECTION:

Changing the mail security level.....	67
Changing the action to take on infected email messages	67
Editing the protection scope of Mail Anti-Virus	67
Scanning compound files that are attached to email messages.....	69
Filtering attachments in email messages	69
Using heuristic analysis.....	70
Scanning emails in Microsoft Office Outlook	70
Scanning emails in The Bat!.....	71

CHANGING THE MAIL SECURITY LEVEL

Mail Anti-Virus applies various groups of settings to protect mail. The settings groups are called *email security levels*. There are three pre-installed email security levels: **High**, **Recommended**, and **Low**. The **Recommended** file security level is considered the optimal setting, and is recommended by Kaspersky Lab.

➤ *To change the email security level:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Mail Anti-Virus**.

In the right part of the window, the settings of the Mail Anti-Virus component are displayed.
3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed email security levels (**High**, **Recommended**, or **Low**), use the slider to select one.
 - If you want to configure a custom email security level, click the **Settings** button and specify settings in the **Mail Anti-Virus** window.

After you configure a custom email security level, the name of the security level in the **Security level** section changes to **Custom**.
 - If you want to change the email security level to **Recommended**, click the **Default** button.
4. To save changes, click the **Save** button.

CHANGING THE ACTION TO TAKE ON INFECTED EMAIL MESSAGES

➤ *To change the action to take on infected email messages:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Mail Anti-Virus**.

In the right part of the window, the settings of the Mail Anti-Virus component are displayed.
3. In the **Action on threat detection** section, select the action that Kaspersky Endpoint Security performs on detection of an infected email message:
 - **Select action automatically.**
 - **Perform action: Disinfect. Delete if disinfection fails.**
 - **Perform action: Disinfect.**
 - **Perform action: Delete.**
 - **Perform action: Block.**
4. To save changes, click the **Save** button.

EDITING THE PROTECTION SCOPE OF MAIL ANTI-VIRUS

The protection scope refers to the objects that the component scans when enabled. The protection scopes of different components have different properties. The properties of the protection scope of Mail Anti-Virus include the settings to

integrate Mail Anti-Virus into email clients, and the type of email messages and the email protocols whose traffic is scanned by Mail Anti-Virus. By default, Kaspersky Endpoint Security scans incoming and outgoing email messages and traffic via the POP3, SMTP, NNTP, and IMAP protocols, and is integrated into the Microsoft Office Outlook and The Bat! email clients.

➤ *To create the protection scope of Mail Anti-Virus:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Mail Anti-Virus**.

In the right part of the window, the settings of the Mail Anti-Virus component are displayed.

3. Click the **Settings** button.

The **General** tab opens in the **Mail Anti-Virus** window.

4. In the **Protection scope** section, do one of the following:

- If you want Mail Anti-Virus to scan all incoming and outgoing email messages on your computer, select the **Incoming and outgoing messages** option.
- If you want Mail Anti-Virus to scan only incoming email messages on your computer, select the **Incoming messages only** option.

If you choose to scan only incoming email messages, we recommend that you perform a one-time scan of all outgoing email messages, because there is a chance of email worms on your computer that spread over electronic mail. This helps to avoid unpleasant situations that result from unmonitored mass emailing of infected messages from your computer.

5. In the **Connectivity** section, do the following:

- If you want Mail Anti-Virus to scan email messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols before they arrive on your computer, select the **POP3 / SMTP / NNTP / IMAP traffic** check box.

If you do not want Mail Anti-Virus to scan email messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols before they arrive on your computer, clear the **POP3 / SMTP / NNTP / IMAP traffic** check box. In this case, messages are scanned by Mail Anti-Virus plug-ins that are embedded in Microsoft Office Outlook and The Bat! after messages arrive on your computer.

If you use an email client other than Microsoft Office Outlook or The Bat!, email messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols are not scanned when the **POP3 / SMTP / NNTP / IMAP traffic** check box is cleared.

If the **Additional: Microsoft Office Outlook plug-in** check box and the **Additional: The Bat! plug-in** check box are cleared, Mail Anti-Virus does not scan email messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols either.

- If you want to open access to Mail Anti-Virus settings from Microsoft Office Outlook and enable scanning of email messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they arrive on the computer by a plug-in that is embedded into Microsoft Office Outlook, select the **Additional: Microsoft Office Outlook plug-in** check box.
- If you want to enable the scanning of email messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they arrive on the computer by a plug-in embedded into The Bat!, select the **Additional: The Bat! plug-in** check box.

If you want to disable the scanning of email messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols after they arrive on the computer by a plug-in embedded into The Bat!, clear the **Additional: The Bat! plug-in** check box.

The Mail Anti-Virus plug-in is embedded in the Microsoft Office Outlook and The Bat! mail programs during installation of Kaspersky Endpoint Security.

6. Click **OK**.
7. To save changes, click the **Save** button.

SCANNING COMPOUND FILES THAT ARE ATTACHED TO EMAIL MESSAGES

➤ *To configure the scanning of compound files that are attached to email messages:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Mail Anti-Virus**.
In the right part of the window, the settings of the Mail Anti-Virus component are displayed.
3. Click the **Settings** button.
The **Mail Anti-Virus** window opens.
4. On the **General** tab, in the **Scan of compound files** section, do the following:
 - If you want Mail Anti-Virus to skip archives that are attached to email messages, clear the **Scan attached archives** check box.
 - If you want Mail Anti-Virus to skip email attachments that are larger than N megabytes in size, select the **Do not scan archives larger than N MB** check box. If you select this check box, specify the maximum archive size in the field that is opposite the name of the check box.
 - If you want Mail Anti-Virus to scan email attachments that take more than N seconds to scan, clear the **Do not scan archives for more than N s** check box.
5. Click **OK**.
6. To save changes, click the **Save** button.

FILTERING ATTACHMENTS IN EMAIL MESSAGES

Malicious programs can be distributed in the form of email attachments. You can configure filtering of email attachments by type, so that files of such types are automatically renamed or deleted.

➤ *To configure filtering of attachments:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Mail Anti-Virus**.
In the right part of the window, the settings of the Mail Anti-Virus component are displayed.
3. In the **Security level** section, click the **Settings** button.

The **Mail Anti-Virus** window opens.

4. In the **Mail Anti-Virus** window, select the **Attachment filter** tab.
5. Do one of the following:
 - If you do not want Mail Anti-Virus to filter email attachments, select the **Disable filtering** setting.
 - If you want Mail Anti-Virus to rename email attachments of the specified types, select the **Rename selected attachment types** setting.
 - If you want Mail Anti-Virus to delete email attachments of the specified types, select the **Delete selected attachment types** setting.
6. Do one of the following:
 - If in step 5 of these instructions you have selected the **Disable filtering** setting, then go to step 7.
 - If in step 5 of these instructions you have selected the **Rename selected attachment types** or the **Delete selected attachment types** setting, the list of file types becomes active. Select the check boxes next to the required file types.

You can change the list of file types by using the **Add**, **Edit**, and **Delete** buttons.
7. Click **OK**.
8. To save changes, click the **Save** button.

USING HEURISTIC ANALYSIS

➔ *To use heuristic analysis:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Mail Anti-Virus**.
In the right part of the window, the settings of the Mail Anti-Virus component are displayed.
3. In the **Security level** section, click the **Settings** button.
The **Mail Anti-Virus** window opens.
4. In the **Mail Anti-Virus** window, select the **Additional** tab.
5. On the **Additional** tab, in the **Scan methods** section, select the **Heuristic Analysis** check box.
6. Use the slider to set the level of detail of the scan during heuristic analysis: **Light scan**, **Medium scan**, or **Deep scan**.
7. Click **OK**.
8. To save changes, click the **Save** button.

SCANNING EMAILS IN MICROSOFT OFFICE OUTLOOK

During installation of Kaspersky Endpoint Security, a special plug-in is embedded into Microsoft Office Outlook. It allows you to open the Mail Anti-Virus settings quickly from inside Microsoft Office Outlook, and to specify at what moment email messages are to be scanned for viruses and other malware. The mail plug-in that is embedded into Microsoft

Office Outlook can scan incoming and outgoing messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols.

Mail Anti-Virus settings can be configured directly in Microsoft Office Outlook if the **Additional: Microsoft Office Outlook plug-in** check box is selected in the interface of Kaspersky Endpoint Security.

In Microsoft Office Outlook, incoming email messages are first scanned by Mail Anti-Virus (when the **POP3 / SMTP / NNTP / IMAP traffic** check box is selected) and then by the mail plug-in that is embedded into Microsoft Office Outlook. If Mail Anti-Virus detects a malicious object in an email message, it alerts you to this event.

Your choice of action in the notification window determines the component that eliminates the threat in the email message: Mail Anti-Virus or the mail plug-in that is embedded into Microsoft Office Outlook.

- If you select **Disinfect** or **Delete** in the notification window of Mail Anti-Virus, threat elimination is performed by Mail Anti-Virus.
- If you select **Skip** in the notification window of Mail Anti-Virus, the mail plug-in that is embedded into Microsoft Office Outlook eliminates the threat.

Outgoing email messages are first scanned by the email plug-in that is embedded into Microsoft Office Outlook, and then by Mail Anti-Virus.

➡ *To adjust the email scan settings in Microsoft Office Outlook:*

1. Open the main Microsoft Outlook application window.
2. Select **Tools** → **Options** from the menu bar.

The **Options** window opens.

3. In the **Options** window, select the **Email protection** tab.

SEE ALSO:

Editing the protection scope of Mail Anti-Virus [67](#)

SCANNING EMAILS IN THE BAT!

During installation of Kaspersky Endpoint Security, a special plug-in is embedded into The Bat!. It allows you to open Mail Anti-Virus settings quickly from inside The Bat!, and to specify at what moment email messages are to be scanned for viruses and other malware. The mail plug-in that is embedded into The Bat! email client can scan incoming and outgoing messages that are transmitted via the POP3, SMTP, NNTP, IMAP, and MAPI protocols.

Mail Anti-Virus settings can be configured directly in The Bat! email client if the **Additional: The Bat! plug-in** check box is selected in the interface of Kaspersky Endpoint Security.

In The Bat!, incoming email messages are first scanned by Mail Anti-Virus (when the **POP3 / SMTP / NNTP / IMAP traffic** check box is selected in the interface of Kaspersky Endpoint Security) and then by the mail plug-in that is embedded into The Bat!. If Mail Anti-Virus detects a malicious object in an email message, it alerts you to this event.

Your choice of action in the notification window determines which component eliminates the threat in the email message: Mail Anti-Virus or the mail plug-in that is embedded into The Bat!.

- If you select **Disinfect** or **Delete** in the notification window, threat elimination will be performed by Mail Anti-Virus.

- If you select **Skip** in the notification window, the email plug-in that is embedded in The Bat! eliminates the threat.

Outgoing email messages are first scanned by the email plug-in that is embedded in The Bat!, and then by Mail Anti-Virus.

The actions that The Bat! performs on infected email messages are defined in the application itself. You can specify the following settings:

- Select the stream of email messages (incoming or outgoing) that is to be scanned.
- Specify the stage when email messages are scanned (before opening an email message, before saving an email message to disk).
- Select the action that The Bat! performs on detection of an infected email message:
 - **Attempt to disinfect infected parts.** If you have selected this option, The Bat! attempts to disinfect infected email messages. If they cannot be disinfected, The Bat! leaves those email messages intact.
 - **Delete infected parts.** If you have selected this option, The Bat! deletes infected or potentially infected email messages.

By default, The Bat! moves all infected email messages to Quarantine without disinfecting them.

The Bat! does not mark infected email messages with a special header.

➡ *To adjust email scan settings in The Bat!:*

1. Open the main The Bat! window.
2. In the **Properties** menu, select **Settings**.
3. Select the **Virus protection** object from the settings tree.

SEE ALSO:

Editing the protection scope of Mail Anti-Virus [67](#)

COMPUTER PROTECTION ON THE INTERNET. WEB ANTI-VIRUS

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

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

IN THIS SECTION:

About Web Anti-Virus	73
Enabling and disabling Web Anti-Virus	73
Configuring Web Anti-Virus	74

ABOUT WEB ANTI-VIRUS

Every time you go online, you expose information that is stored on your computer to viruses and other malware. They can infiltrate your computer while you are downloading free software or browsing websites that are compromised by hacker attacks. Network worms can find a way onto your computer as soon as you establish an Internet connection, even before you open a web page or download a file.

Web Anti-Virus protects incoming and outgoing data that is sent to and from the computer over the HTTP and FTP protocols and checks URLs against the list of suspicious or phishing web addresses.

Web Anti-Virus intercepts and analyzes for viruses and other malware every web page or file that is accessed by the user or an application via the HTTP or FTP protocol:

- If the page or file is found not to contain malicious code, the user gains immediate access to them.
- If the web page or the file which the user attempts to access contains malicious code, the application takes the action on the object that is specified in the settings of Web Anti-Virus (see the section "Changing the action to take on malicious web traffic objects" on page [76](#)).

Web Anti-Virus does not support protocols that ensure encrypted data transfer.

ENABLING AND DISABLING WEB ANTI-VIRUS

By default, Web Anti-Virus is enabled, running in a mode that is recommended by Kaspersky Lab's experts. You can disable Web Anti-Virus, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➤ *To enable or disable Web Anti-Virus on the Protection and Control tab of the main application window:*



1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.

The **Protection** section opens.



4. Right-click to bring up the context menu of the line with information about the Web Anti-Virus component.
A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable Web Anti-Virus, select **Enable** in the menu.

The component status icon , which is displayed on the left in the **Web Anti-Virus** line, changes to the icon .

- To disable Web Anti-Virus, select **Disable** in the menu.

The component status icon , which is displayed on the left in the **Web Anti-Virus** line, changes to the icon .

➤ *To enable or disable Web Anti-Virus from the application settings window:*

1. Open the application settings window.
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.
In the right part of the window, the settings of the Web Anti-Virus component are displayed.
3. Do one of the following:
 - If you want to enable Web Anti-Virus, select the **Enable Web Anti-Virus** check box.
 - If you want to disable Web Anti-Virus, clear the **Enable Web Anti-Virus** check box.
4. To save changes, click the **Save** button.

CONFIGURING WEB ANTI-VIRUS

You can do the following to configure Web Anti-Virus:

- Change web traffic security level.

You can select one of the pre-installed security levels for web traffic that is received or transmitted via the HTTP and FTP protocols, or configure a custom web traffic security level.

If you change the web traffic security level settings, you can always revert to the recommended web traffic security level settings.

- Change the action that Kaspersky Endpoint Security performs on infected web traffic objects.

If analysis of an HTTP object shows that it contains malicious code, the response by Web Anti-Virus depends on the action that you have specified.

- Configure Web Anti-Virus scanning of links against databases of phishing and suspicious URLs.
- Configure use of heuristic analysis when scanning web traffic for viruses and other malicious programs.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of applications in the operating system. Heuristic analysis can detect new threats for which there are currently no records in the Kaspersky Endpoint Security databases.

- Configure use of heuristic analysis when scanning web pages for phishing links.
- Optimize Web Anti-Virus scanning of web traffic that is sent and received via the HTTP and FTP protocols.
- Create a list of trusted URLs.

You can create a list of URLs whose content you trust. Web Anti-Virus does not analyze information from trusted URLs for viruses or other threats. This option may be useful, for example, when Web Anti-Virus interferes with downloading a file from a known website.

A URL may be the address of a specific web page or the address of a website.

IN THIS SECTION:

Changing the web traffic security level.....	75
Changing the action to take on malicious web traffic objects	76
Scanning URLs against databases of suspicious and phishing web addresses	76
Using Heuristic Analyzer with Web Anti-Virus.....	77
Configuring the duration of caching web traffic	77
Editing the list of trusted URLs.....	78

CHANGING THE WEB TRAFFIC SECURITY LEVEL

To protect data that is received and transmitted via the HTTP and FTP protocols, Web Anti-Virus applies various settings groups. Such settings groups are called *web traffic security levels*. There are three pre-installed web traffic security levels: **High**, **Recommended**, and **Low**. The **Recommended** web traffic security level is considered the optimal setting, and is recommended by Kaspersky Lab.

➔ *To change the web traffic security level:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.
In the right part of the window, the settings of the Web Anti-Virus component are displayed.
3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed web traffic security levels (**High**, **Recommended**, or **Low**), use the slider to select one.
 - If you want to configure a custom web traffic security level, click the **Settings** button and specify settings in the **Web Anti-Virus** window.

When you have configured a custom web traffic security level, the name of the security level in the **Security level** section changes to **Custom**.

- If you want to change the web traffic security level to **Recommended**, click the **Default** button.
4. To save changes, click the **Save** button.

CHANGING THE ACTION TO TAKE ON MALICIOUS WEB TRAFFIC OBJECTS

➤ *To change the action to take on malicious web traffic objects:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.

In the right part of the window, the settings of the Web Anti-Virus component are displayed.
3. In the **Action on threat detection** section, select the action that Kaspersky Endpoint Security performs on malicious web traffic objects:
 - **Select action automatically.**
 - **Block download.**
 - **Allow download.**
4. To save changes, click the **Save** button.

SCANNING URLs AGAINST DATABASES OF SUSPICIOUS AND PHISHING WEB ADDRESSES

Scanning links to see if they are included in the list of phishing web addresses allows avoiding *phishing attacks*. A phishing attack can be disguised, for example, as an email message from your bank with a link to the official website of the bank. By clicking the link, you go to an exact copy of the bank's website and can even see its real web address in the browser, even though you are on a counterfeit site. From this point forward, all of your actions on the site are tracked and can be used to steal your money.

Because links to phishing websites may be received not only in an email message, but also from other sources such as ICQ messages, Web Anti-Virus monitors attempts to access a phishing website on the level of web traffic and blocks access to such sites. Lists of phishing URLs are included with the Kaspersky Endpoint Security distribution kit.

➤ *To configure Web Anti-Virus to check URLs against the databases of suspicious and phishing web addresses:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.

In the right part of the window, the settings of the Web Anti-Virus component are displayed.
3. Click the **Settings** button.

The **Web Anti-Virus** window opens.
4. In the **Web Anti-Virus** window, select the **General** tab.
5. In the **Scan methods** section:

- If you want Web Anti-Virus to check URLs against the databases of suspicious web addresses, select the **Check if URLs are listed in the database of suspicious URLs** check box.
- If you want Web Anti-Virus to check URLs against the databases of phishing web addresses, select the **Check if URLs are listed in the database of phishing URLs** check box.

You can also check URLs against the reputation databases of Kaspersky Security Network (see the section "Participating in Kaspersky Security Network" on page [237](#)).

6. Click **OK**.
7. To save changes, click the **Save** button.

USING HEURISTIC ANALYZER WITH WEB ANTI-VIRUS

➔ *To configure the use of heuristic analysis:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.
In the right part of the window, the settings of the Web Anti-Virus component are displayed.

3. In the **Security level** section, click the **Settings** button.

The **Web Anti-Virus** window opens.

4. In the **Web Anti-Virus** window, select the **General** tab.
5. In the **Scan methods** section:
 - If you want Web Anti-Virus to use heuristic analysis to scan web traffic for viruses and other malicious programs, select the **Heuristic analysis for detecting viruses** check box and use the slider to set the level of detail of heuristic analysis: **light scan**, **medium scan**, or **deep scan**.
 - If you want Web Anti-Virus to use heuristic analysis to scan web pages for phishing links, select the **Heuristic analysis for detecting phishing links** check box and use the slider to set the level of detail of heuristic analysis: **light scan**, **medium scan**, or **deep scan**.
6. Click **OK**.
7. To save changes, click the **Save** button.

CONFIGURING THE DURATION OF CACHING WEB TRAFFIC

To detect malicious code more efficiently, Web Anti-Virus caches fragments of objects that are downloaded from the Internet. Web Anti-Virus uses caching to scan objects only after they arrive on the computer in full.

Caching objects increases object processing time, and therefore the time before the application delivers the object to the user. Caching can cause problems when downloading or processing large objects, because the connection with the HTTP client may time out.

To solve this problem, you can limit the duration for which fragments of objects that are downloaded from the Internet are cached. When the specified period of time expires, the user receives the downloaded part of the object without scanning, and after the object is fully copied, the object is scanned in full. This allows reducing the time that is needed to deliver objects to the user and eliminating the disconnection problem. The Internet security level is not reduced in that case.

Removing the limit on caching time makes anti-virus scanning more efficient, but slightly slows down access to objects.

➤ *To configure web traffic caching time:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.

In the right part of the window, the settings of the Web Anti-Virus component are displayed.
3. Click the **Settings** button.

The **Web Anti-Virus** window opens.
4. In the **Web Anti-Virus** window, select the **General** tab.
5. In the **Additional** section, do one of the following:
 - If you want to limit the time for which web traffic is cached and speed up its scanning, select the **Limit web traffic caching time** check box.
 - If you want to cancel the time limit on caching web traffic, clear the **Limit web traffic caching time** check box.
6. Click **OK**.
7. To save changes, click the **Save** button.

EDITING THE LIST OF TRUSTED URLS

➤ *To create a list of trusted URLs:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Web Anti-Virus**.

In the right part of the window, the settings of the Web Anti-Virus component are displayed.
3. Click the **Settings** button.

The **Web Anti-Virus** window opens.
4. Select the **Trusted URLs** tab.
5. Select the **Do not scan web traffic from trusted URLs** check box.

6. Create a list of URLs / web pages whose content you trust. To do so:
 - a. Click the **Add** button.
The **Address / Address mask** window opens.
 - b. Enter the address of the website / web page or the address mask of the website / web page.
 - c. Click **OK**.
A new record appears in the list of trusted URLs.
 - d. If necessary, repeat steps a–c of the instructions.
7. Click **OK**.
8. To save changes, click the **Save** button.

PROTECTION OF INSTANT MESSAGING CLIENT TRAFFIC. IM ANTI-VIRUS

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

This section contains information about IM Anti-Virus and instructions on how to configure the component settings.

IN THIS SECTION:

About IM Anti-Virus	80
Enabling and disabling IM Anti-Virus.....	80
Configuring IM Anti-Virus	81

ABOUT IM ANTI-VIRUS

IM Anti-Virus scans the traffic of instant messaging clients (so-called *Internet pagers*).

Messages that are sent through IM clients can contain the following kinds of security threats:

- URLs that attempt to download a malicious program to the computer
- URLs to malicious programs and websites that intruders use for phishing attacks

Phishing attacks aim to steal personal user data, such as credit card numbers, passport details, passwords for bank payment systems and other online services (such as social networking sites or email accounts).

Files can be transmitted through IM clients. When you attempt to save such files, they are scanned by the File Anti-Virus component (see the section "About File Anti-Virus" on page [51](#)).

IM Anti-Virus intercepts every message that the user sends or receives through an IM client and scans it for objects that may threaten computer security:

- If no threats are detected in the message, it becomes available to the user.
- If threats are detected in the message, IM Anti-Virus replaces the message with information about the threat in the message window of the active instant messenger.

IM Anti-Virus does not support protocols that provide encrypted data transfer. IM Anti-Virus does not scan traffic of IM messengers that use a secure connection.

ENABLING AND DISABLING IM ANTI-VIRUS

By default, IM Anti-Virus is enabled, running in a mode that is recommended by Kaspersky Lab's experts. You can disable IM Anti-Virus, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window
- From the application settings window (see the section "Application settings window" on page [48](#))



➔ *To enable or disable IM Anti-Virus on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.



The **Protection** section opens.

4. Right-click the **IM Anti-Virus** line to display the context menu of component actions.
5. Do one of the following:

- To enable IM Anti-Virus, select **Enable** in the context menu.

The component status icon , which is displayed on the left in the **IM Anti-Virus** line, changes to the icon .

- To disable IM Anti-Virus, select **Disable** in the context menu.

The component status icon , which is displayed on the left in the **IM Anti-Virus** line, changes to the icon .

➔ *To enable or disable IM Anti-Virus from the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **IM Anti-Virus**.

In the right part of the window, the settings of the IM Anti-Virus component are displayed.

3. Do one of the following:
 - If you want to enable IM Anti-Virus, select the **Enable IM Anti-Virus** check box.
 - If you want to disable IM Anti-Virus, clear the **Enable IM Anti-Virus** check box.
4. To save changes, click the **Save** button.

CONFIGURING IM ANTI-VIRUS

You can perform the following actions to configure IM Anti-Virus:

- Create the protection scope.

You can expand or narrow the protection scope by modifying the type of IM client messages that are scanned.

- Configure IM Anti-Virus scanning of URLs in IM client messages against databases of suspicious and phishing URLs.
- Configure Heuristic Analyzer.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of applications in the operating system. Heuristic analysis can detect new threats in IM client messages for which there are currently no records in the Kaspersky Endpoint Security databases.

IN THIS SECTION:

Creating the protection scope of IM Anti-Virus	82
Scanning URLs against databases of suspicious and phishing URLs with IM Anti-Virus.....	82
Using Heuristic Analyzer with IM Anti-Virus	83

CREATING THE PROTECTION SCOPE OF IM ANTI-VIRUS

The protection scope refers to the objects that the component scans when enabled. The protection scopes of different components have different properties. The type of scanned IM client messages, incoming or outgoing, is a property of the IM Anti-Virus protection scope. By default, IM Anti-Virus scans both incoming and outgoing messages. You may disable scanning of outgoing traffic.

➤ *To create the protection scope:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **IM Anti-Virus**.

In the right part of the window, the settings of the IM Anti-Virus component are displayed.
3. In the **Protection scope** section, do one of the following:
 - If you want IM Anti-Virus to scan all incoming and outgoing IM client messages, select the **Incoming and outgoing messages** option.
 - If you want IM Anti-Virus to check only incoming IM client messages, select the **Incoming messages only** option.
4. To save changes, click the **Save** button.

SCANNING URLs AGAINST DATABASES OF SUSPICIOUS AND PHISHING URLs WITH IM ANTI-VIRUS

➤ *To configure IM Anti-Virus to check URLs against the databases of suspicious and phishing web addresses:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **IM Anti-Virus**.

In the right part of the window, the settings of the IM Anti-Virus component are displayed.
3. In the **Scan methods** section, select the methods that you want IM Anti-Virus to use:
 - If you want to check URLs in IM client messages against the database of suspicious URLs, select the **Check if URLs are listed in the database of suspicious URLs** check box.
 - If you want to check URLs in IM client messages against the database of phishing URLs, select the **Check if URLs are listed in the database of phishing URLs** check box.

4. To save changes, click the **Save** button.

USING HEURISTIC ANALYZER WITH IM ANTI-VIRUS

➤ *To configure the use of Heuristic Analyzer in the operation of IM Anti-Virus:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **IM Anti-Virus**.
In the right part of the window, the settings of the IM Anti-Virus component are displayed.
3. In the **Scan methods** section:
 - a. Select the **Heuristic analysis** check box.
 - b. Use the slider to set the level of detail of Heuristic Analysis: **Light scan**, **Medium scan** or **Deep scan**.
4. To save changes, click the **Save** button.

NETWORK PROTECTION

This section describes the operating principles and configuration of the Firewall and Network Attack Blocker components, and of network traffic control.

IN THIS SECTION:

Firewall.....	84
Network Attack Blocker	104
Monitoring network traffic	106
Network Monitor	110

FIREWALL

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

IN THIS SECTION:

About Firewall	84
Enabling or disabling Firewall.....	85
About network rules	85
About the network connection status	86
Changing the network connection status.....	86
Managing network packet rules.....	87
Managing network rules for application groups	91
Managing network rules for applications	98
Configuring advanced Firewall settings.....	103

ABOUT FIREWALL

During use on LANs and the Internet, a computer is exposed to viruses, other malware, and a variety of attacks that exploit vulnerabilities in operating systems and software.

Firewall protects personal data that is stored on the user's computer, blocking all kinds of threats to the operating system while the computer is connected to the Internet or a local area network. Firewall detects all network connections of the user's computer and provides a list of IP addresses, with an indication of the status of the default network connection.

The Firewall component filters all network activity according to network rules (see the section "About network rules" on page [85](#)). Configuring network rules lets you specify the desired level of computer protection, from blocking Internet access for all applications to allowing unlimited access.

ENABLING OR DISABLING FIREWALL

By default, Firewall is enabled and functions in the optimal mode. If needed, you can disable Firewall.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))



➔ *To enable or disable Firewall on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.



The **Protection** section opens.

4. Right-click the **Firewall** line to open the context menu of Firewall actions.
5. Do one of the following:

- To enable Firewall, in the context menu, select **Enable**.

The component status icon , which is displayed on the left in the **Firewall** line, changes to the icon .

- To disable Firewall, select **Disable** in the context menu.

The component status icon , which is displayed on the left in the **Firewall** line, changes to the icon .

➔ *To enable or disable Firewall, in the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Do one of the following:
 - To enable Firewall, select the **Enable Firewall** check box.
 - To disable Firewall, select the **Disable Firewall** check box.
4. To save changes, click the **Save** button.

ABOUT NETWORK RULES

Network rules are allowed or blocked actions that are performed by Firewall on detecting a network connection attempt.

Firewall provides protection against network attacks of different kinds at two levels: the network level and the program level. Protection at the network level is provided by applying network packet rules. Protection at the program level is provided by applying rules by which installed applications can access network resources.

Based on the two levels of Firewall protection, you can create:

- **Network packet rules:** Network packet rules impose restrictions on network packets, regardless of the program. Such rules restrict inbound and outbound network traffic through specific ports of the selected data protocol. Firewall specifies certain network packet rules by default.
- **Application network rules:** Application network rules impose restrictions on the network activity of 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.

Network packet rules have a higher priority than network rules for applications. If both network packet rules and network rules for applications are specified for the same type of network activity, the network activity is handled according to the network packet rules.

You can specify an execution priority for each network packet rule and each network rule for applications.

ABOUT THE NETWORK CONNECTION STATUS

Firewall controls all network connections on the user's computer and automatically assigns a status to each detected network connection.

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). When the user operates 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. Firewall permits any network activity within networks with this status.

CHANGING THE NETWORK CONNECTION STATUS

➡ *To change the network connection status:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Available networks** button.

The **Firewall** window opens under the **Networks** tab.

4. On the **Networks** tab, select a network connection whose status you want to change.
5. Right-click to display the context menu of the network connection.
6. In the context menu, select network connection status (see the section "About the network connection status" on page [86](#)):

- **Public network**
 - **Local network**
 - **Trusted network**
7. In the **Firewall** window, click **OK**.
 8. To save changes, click the **Save** button.

MANAGING NETWORK PACKET RULES

You can perform the following actions while managing network packet rules:

- Create a new network packet rule.

You can create a new network packet rule by creating a set of conditions and actions that is applied to network packets and data streams.

- Enable or disable a network packet rule.

All network packet rules that are created by Firewall by default have *Enabled* status. When a network packet rule is enabled, Firewall applies this rule.

You can disable any network packet rule that is selected in the list of network packet rules. When a network packet rule is disabled, Firewall temporarily does not apply this rule.

A new custom network packet rule is added to the list of network packet rules by default with *Enabled* status.

- Edit the settings of an existing network packet rule.

After you create a new network packet rule, you can always return to editing its settings and modify them as needed.

- Change the Firewall action for a network packet rule.

In the list of network packet rules, you can edit the action that is taken by Firewall on detecting network activity that matches a specific network packet rule.

- Change the priority of a network packet rule.

You can raise or lower the priority of a network packet rule that is selected in the list.

- Remove a network packet rule.

You can remove a network packet rule to stop Firewall from applying this rule on detecting network activity and to stop this rule from showing in the list of network packet rules with *Disabled* status.


IN THIS SECTION:

Creating and editing a network packet rule	88
Enabling or disabling a network packet rule	90
Changing the Firewall action for a network packet rule	90
Changing the priority of a network packet rule	91

CREATING AND EDITING A NETWORK PACKET RULE

When creating network packet rules, remember that they have priority over network rules for applications.

➔ To create or edit a network packet rule:

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Network packet rules** button.
The **Firewall** window opens to the **Network packet rules** tab.
This tab shows a list of default network packet rules that are set by Firewall.
4. Do one of the following:
 - To create a new network packet rule, click the **Add** button.
 - To edit a network packet rule, select it in the list of network packet rules and click the **Edit** button.
5. The **Network rule** window opens.
6. In the **Action** drop-down list, select the action to be performed by Firewall on detecting this kind of network activity:
 - **Allow**
 - **Block**
 - **By application rules.**
7. In the **Name** field, specify the name of the network service in one of the following ways:
 - Click the  icon to the right of the **Name** field and select the name of the network service in the drop-down list.
Kaspersky Endpoint Security includes network services that match the most frequently used network connections.
 - Type the name of the network service in the **Name** field manually.

A *network service* is a collection of settings that describe the network activity for which you create a network rule.
8. Specify the data transfer protocol:
 - a. Select the **Protocol** check box.
 - b. In the drop-down list, select the type of protocol for which network activity is to be monitored.
Firewall monitors network connections that use the TCP, UDP, ICMP, ICMPv6, IGMP, and GRE protocols.
By default, the **Protocol** check box is cleared.

If you select a network service from the **Name** drop-down list, the **Protocol** check box is selected automatically and the drop-down list next to the check box is filled with a protocol type that corresponds to the selected network service.

9. In the **Direction** drop-down list, select the direction of the monitored network activity.

Firewall monitors network connections with the following directions:

- **Inbound**
 - **Inbound (stream)**
 - **Inbound / Outbound**
 - **Outbound**
 - **Outbound (stream)**
10. If ICMP or ICMPv6 is selected as the protocol, you can specify the ICMP packet type and code:
 - a. Select the **ICMP type** check box and select the ICMP packet type in the drop-down list.
 - b. Select the **ICMP code** check box and select the ICMP packet code in the drop-down list.
 11. If TCP or UDP is selected as the protocol, you can specify the ports of the local and remote computers between which the connection is to be monitored:
 - a. Type the ports of the remote computer in the **Remote ports** field.
 - b. Type the ports of the local computer in the **Local ports** field.
 12. Specify the network address in the **Address** field, if necessary.

You can use an IP address as a network address or specify the status of the network connection. In the latter case, network addresses are obtained from all active network connections that have the selected status.

You can select one of the following network address categories:

- **Any address**
 - **Subnet address**
 - **Addresses from the list**
13. If you want the allow or block actions of the network rule to be reflected in the report, select the **Log event** check box (see the section "Managing reports" on page [193](#)).

14. In the **Network rule** window, click **OK**.

If you create a new network rule, the rule is displayed on the **Network packet rules** tab of the **Firewall** window. By default, the new network rule is placed at the end of the list of network packet rules.

15. In the **Firewall** window, click **OK**.
16. To save changes, click the **Save** button.

ENABLING OR DISABLING A NETWORK PACKET RULE

➔ *To enable or disable a network packet rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Network packet rules** button.

The **Firewall** window opens to the **Network packet rules** tab.

4. In the list of network packet rules, select the desired network packet rule.
5. Do one of the following:
 - To enable the rule, select the check box next to the name of the network packet rule.
 - To disable the rule, clear the check box next to the name of the network packet rule.
6. Click **OK**.
The **Firewall** window closes.
7. To save changes, click the **Save** button.

CHANGING THE FIREWALL ACTION FOR A NETWORK PACKET RULE

➔ *To change the Firewall action that is applied to a network packet rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Network packet rules** button.
The **Firewall** window opens to the **Network packet rules** tab.
4. In the list of network packet rules, select the network packet rule whose action you want to change.
5. In the **Permission** column, right-click to bring up the context menu and select the action that you want to assign:
 - **Allow**
 - **Block**

- According to the application rule.
 - Log events.
6. In the **Firewall** window, click **OK**.
The **Firewall** window closes.
 7. To save changes, click the **Save** button.

CHANGING THE PRIORITY OF A NETWORK PACKET RULE

The priority of a network packet rule is determined by its position in the list of network packet rules. The topmost network packet rule in the list of network packet rules has the highest priority.

Every manually created network packet rule is added to the end of the list of network packet rules and is of the lowest priority.

Firewall executes rules in the order in which they appear in the list of network packet rules, from top to bottom. According to each processed network packet rule that applies to a particular network connection, Firewall either allows or blocks network access to the address and port that are specified in the settings of this network connection.

➔ *To change the network packet rule priority:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Network packet rules** button.
The **Firewall** window opens to the **Network packet rules** tab.
4. In the list of network packet rules, select the network packet rule whose priority you want to change.
5. Use the **Up** and **Down** buttons to move the network packet rule to the desired spot in the list of network packet rules.
6. Click **OK**.
7. The **Firewall** window closes.
8. To save changes, click the **Save** button.

MANAGING NETWORK RULES FOR APPLICATION GROUPS

By default, Kaspersky Endpoint Security groups all applications that are installed on the computer by the name of the vendor of the software whose file or network activity it monitors. Application groups are in turn categorized into trust groups. All applications and application groups inherit properties from their parent group: application control rules, application network rules, and their execution priority.

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 danger that the applications pose to the operating system.

The trust groups are as follows:

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

No operations are prohibited for these applications.

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

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

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

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

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

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

By default, the Firewall component applies the network rules for an application group when filtering the network activity of all applications within the group, similarly to the Application Privilege Control component (see page [125](#)). The application group network rules define the rights of applications within the group to access different network connections.

By default, Firewall creates a set of network rules for each application group that is detected by Kaspersky Endpoint Security on the computer. You can change the Firewall action that is applied to the application group network rules that are created by default. You cannot edit, remove, disable, or change the priority of application group network rules that are created by default.

You can perform the following actions while managing the application group network rules:

- Create a new application group network rule.

You can create a new network rule for an application group, according to which Firewall regulates the network activity of applications that belong to this group.

- Enable or disable an application group network rule.

All network rules for an application group are added to the list of network rules for the application group with *Enabled* status. When an application group network rule is enabled, Firewall applies this rule.

You can disable a custom network rule for an application group. When a network rule for an application group is disabled, Firewall does not apply this rule temporarily.

- Edit the settings of an application group network rule.

After you create a new application group network rule, you can always return to editing its settings and modify them as needed.

- Change the Firewall action that is applied to an application group network rule.

In the list of network rules for an application group, you can edit the action that Firewall applies for the application group network rule on detecting network activity in this application group.

- Change the priority of an application group network rule.

You can raise or lower the priority of a custom network rule for an application group.

- Remove an application group network rule.

You can remove a custom rule for an application group to stop Firewall from applying this network rule to the selected application group on detecting network activity, and to stop this rule from appearing in the list of network rules for the application group.

IN THIS SECTION:

Creating and editing an application group network rule	93
Enabling or disabling an application group network rule	95
Changing the Firewall action for an application group network rule	96
Changing the priority of an application group network rule.....	97

CREATING AND EDITING AN APPLICATION GROUP NETWORK RULE

➤ *To create or edit a network rule for an application group:*


1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. In the list of applications, select the group of applications for which you want to create or edit a network rule.
5. Right-click to bring up the context menu and select the **Group rules** item.

The **Application group control rules** window opens.

6. In the **Application group control rules** window that opens, select the **Network rules** tab.
7. Do one of the following:
 - To create a new network rule for an application group, click the **Add** button.
 - To edit a network rule for an application group, select it in the list of network rules and click the **Edit** button.
8. The **Network rule** window opens.
9. In the **Action** drop-down list, select the action to be performed by Firewall on detecting this kind of network activity:
 - **Allow**
 - **Block**
10. In the **Name** field, specify the name of the network service in one of the following ways:

- Click the  icon to the right of the **Name** field and select the name of the network service in the drop-down list.

Kaspersky Endpoint Security includes network services that match the most frequently used network connections.

- Type the name of the network service in the **Name** field manually.

A *network service* is a collection of settings that describe the network activity for which you create a network rule.

11. Specify the data transfer protocol:
 - a. Select the **Protocol** check box.
 - b. In the drop-down list, select the type of protocol on which to monitor network activity.

Firewall monitors network connections that use the TCP, UDP, ICMP, ICMPv6, IGMP, and GRE protocols.

By default, the **Protocol** check box is cleared.

If you select a network service from the **Name** drop-down list, the **Protocol** check box is selected automatically and the drop-down list next to the check box is filled with a protocol type that corresponds to the selected network service.

12. In the **Direction** drop-down list, select the direction of the monitored network activity.

Firewall monitors network connections with the following directions:

- **Inbound**
- **Inbound (stream)**
- **Inbound / Outbound**

- **Outbound**
 - **Outbound (stream)**
13. If ICMP or ICMPv6 is selected as the protocol, you can specify the ICMP packet type and code:
 - a. Select the **ICMP type** check box and select the ICMP packet type in the drop-down list.
 - b. Select the **ICMP code** check box and select the ICMP packet code in the drop-down list.
 14. If TCP or UDP is selected as the protocol type, you can specify the ports of the local and remote computers between which the connection is to be monitored:
 - a. Type the ports of the remote computer in the **Remote ports** field.
 - b. Type the ports of the local computer in the **Local ports** field.
 15. Specify the network address in the **Address** field, if necessary.

You can use an IP address as a network address or specify the status of the network connection. In the latter case, network addresses are obtained from all active network connections that have the selected status.

You can select one of the following network address categories:

- **Any address**
 - **Subnet address**
 - **Addresses from the list**
16. If you want the allow or block actions of the network rule to be reflected in the report, select the **Log event** check box (see the section "Managing reports" on page [193](#)).
 17. In the **Network rule** window, click **OK**.

If you create a new network rule for an application group, the rule is displayed on the **Network rules** tab of the **Application group control rules** window.
 18. In the **Application group control rules** window, click **OK**.
 19. In the **Firewall** window, click **OK**.
 20. To save changes, click the **Save** button.

ENABLING OR DISABLING AN APPLICATION GROUP NETWORK RULE

➔ *To enable or disable an application group network rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.
4. In the list of applications, select the desired application group.
5. Right-click to bring up the context menu and select the **Group rules** item.

The **Application group control rules** window opens.

6. Select the **Network rules** tab.
7. In the list of network rules for application groups, select the desired network rule.
8. Do one of the following:
 - To enable the rule, select the check box next to the name of the application group network rule.
 - To disable the rule, clear the check box next to the application group network rule name.

You cannot disable an application group network rule that is created by Firewall by default.

9. In the **Application group control rules** window, click **OK**.
10. In the **Firewall** window, click **OK**.
11. To save changes, click the **Save** button.

CHANGING THE FIREWALL ACTION FOR AN APPLICATION GROUP NETWORK RULE

You can change the Firewall action that is applied to network rules for an entire application group that were created by default, and change the Firewall action for a single custom application group network rule.

➤ *To modify the Firewall response for network rules for an entire application group:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. To change the Firewall action that is applied to all network rules that are created by default, in the list of applications, select an application group. The custom network rules for an application group remain unchanged.
5. In the **Network** column, click to display the context menu and select the action that you want to assign:
 - **Inherit**
 - **Allow**
 - **Block**
6. Click **OK**.
7. To save changes, click the **Save** button.

➤ *To modify the Firewall response for one application group network rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the settings of the Firewall component are displayed.

3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. In the list of applications, select the desired application group.
5. Right-click to bring up the context menu and select the **Group rules** item.

The **Application group control rules** window opens.

6. In the **Application group control rules** window that opens, select the **Network rules** tab.
7. In the list of application group network rules, select the network rule for which you want to change the Firewall action.
8. In the **Permission** column, right-click to bring up the context menu and select the action that you want to assign:
 - **Allow**
 - **Block**
 - **Log events**
9. In the **Application group control rules** window, click **OK**.
10. In the **Firewall** window, click **OK**.
11. To save changes, click the **Save** button.

CHANGING THE PRIORITY OF AN APPLICATION GROUP NETWORK RULE

The priority of an application group network rule is determined by its position in the list of network rules. Firewall executes the rules in the order in which they appear in the list of network rules, from top to bottom. According to each processed network rule that applies to a particular network connection, Firewall either allows or blocks network access to the address and port that are indicated in the settings of this network connection.

Custom application group network rules have a higher priority than default application group network rules.

➤ *You cannot change the priority of default application group network rules. To change the priority of an application group network rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.
The **Firewall** window opens to the **Application control rules** tab.
4. In the list of applications, select the desired application group.
5. Right-click to bring up the context menu and select the **Group rules** item.
The **Application group control rules** window opens.
6. In the **Application group control rules** window that opens, select the **Network rules** tab.

7. In the list of application group network rules, select the network rule whose priority you want to change.
8. Use the **Up** and **Down** buttons to move the application group network rule to the desired spot in the list of application group network rules.
9. In the **Application group control rules** window, click **OK**.
10. In the **Firewall** window, click **OK**.
11. To save changes, click the **Save** button.

MANAGING NETWORK RULES FOR APPLICATIONS

Firewall uses the application network rules to regulate the access of applications to different network connections.

By default, Firewall creates a set of network rules for each application group that Kaspersky Endpoint Security detects on the computer. Applications that belong to this application group inherit these network rules. You can change the Firewall action for inherited application network rules. You cannot edit, remove, disable, or change the priority of the application network rules that are inherited from the parent group of applications.

You can perform the following actions while managing application network rules:

- Create a new application network rule.

You can create a new application network rule that Firewall uses in regulating the network activity of the given application.

- Enable or disable an application network rule.

All application network rules are added to the list of application network rules with *Enabled* status. When an application network rule is enabled, Firewall applies this rule.

You can disable any custom application network rule. When an application network rule is disabled, Firewall temporarily does not apply this rule.

- Edit the settings of an application network rule.

After you create a new application network rule, you can always return to editing its settings and modify them as needed.

- Change the Firewall action for an application network rule.

In the list of application network rules, you can change the Firewall action that is applied on detecting network activity of the given application.

- Change the priority of an application network rule.

You can raise or lower the priority of a custom application network rule.

- Remove an application network rule.


You can remove a custom application network rule to stop Firewall from applying this network rule to the selected application on detecting network activity and to stop this rule from showing in the list of application network rules.

IN THIS SECTION:

Creating and editing an application network rule.....	99
Enabling or disabling an application network rule	101
Changing the Firewall action for an application network rule	101
Changing the priority of an application network rule.....	103

CREATING AND EDITING AN APPLICATION NETWORK RULE

➔ *To create or edit a network rule for an application:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.
The **Firewall** window opens to the **Application control rules** tab.
4. In the list of applications, select the application for which you want to create or edit a network rule.
5. Right-click to bring up the context menu and select **Application rules**.
The **Application control rules** window opens.
6. In the **Application control rules** window that opens, select the **Network rules** tab.
7. Do one of the following:
 - To create a new network rule for an application, click the **Add** button.
 - To edit a network rule for an application, select it in the list of network rules and click the **Edit** button.
8. The **Network rule** window opens.
9. In the **Action** drop-down list, select the action to be performed by Firewall on detecting this kind of network activity:
 - **Allow**
 - **Block**
10. In the **Name** field, specify the name of the network service in one of the following ways:
 - Click the  icon to the right of the **Name** field and select the name of the network service in the drop-down list.

Kaspersky Endpoint Security includes network services that match the most frequently used network connections.
 - Type the name of the network service in the **Name** field manually.

A *network service* is a collection of settings that describe the network activity for which you create a network rule.

11. Specify the data transfer protocol:

- a. Select the **Protocol** check box.
- b. In the drop-down list, select the type of protocol on which to monitor network activity.

Firewall monitors network connections that use the TCP, UDP, ICMP, ICMPv6, IGMP, and GRE protocols.

By default, the **Protocol** check box is cleared.

If you select a network service from the **Name** drop-down list, the **Protocol** check box is selected automatically and the drop-down list next to the check box is filled with a protocol type that corresponds to the selected network service.

12. In the **Direction** drop-down list, select the direction of the monitored network activity.

Firewall monitors network connections with the following directions:

- **Inbound**
- **Inbound (stream)**
- **Inbound / Outbound**
- **Outbound**
- **Outbound (stream)**

13. If ICMP or ICMPv6 is selected as the protocol, you can specify the ICMP packet type and code:

- a. Select the **ICMP type** check box and select the ICMP packet type in the drop-down list.
- b. Select the **ICMP code** check box and select the ICMP packet code in the drop-down list.

14. If TCP or UDP is selected as the protocol, you can specify the ports of the local and remote computers between which the connection is to be monitored:

- a. Type the ports of the remote computer in the **Remote ports** field.
- b. Type the ports of the local computer in the **Local ports** field.

15. Specify the network address in the **Address** field, if necessary.

You can use an IP address as a network address or specify the status of the network connection. In the latter case, network addresses are obtained from all active network connections that have the selected status.

You can select one of the following network address categories:

- **Any address**
- **Subnet address**
- **Addresses from the list**

16. If you want the allow or block actions of the network rule to be reflected in the report, select the **Log event** check box (see the section "Managing reports" on page [193](#)).

17. In the **Network rule** window, click **OK**.

If you create a new network rule for an application, the rule is displayed on the **Network rules** tab of the **Application rules** window.

18. In the **Application control rules** window, click **OK**.
19. In the **Firewall** window, click **OK**.
20. To save changes, click the **Save** button.

ENABLING OR DISABLING AN APPLICATION NETWORK RULE

➤ *To enable or disable an application network rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. In the list of applications, select the desired application.
5. Right-click to bring up the context menu and select **Application rules**.

The **Application control rules** window opens.

6. Select the **Network rules** tab.
7. In the list of application network rules, select the desired application network rule.
8. Do one of the following:
 - To enable the rule, select the check box next to the name of the application network rule.
 - To disable the rule, clear the check box next to the name of the application network rule.

You cannot disable an application network rule that is created by Firewall by default.

9. In the **Application control rules** window, click **OK**.
10. In the **Firewall** window, click **OK**.
11. To save changes, click the **Save** button.

CHANGING THE FIREWALL ACTION FOR AN APPLICATION NETWORK RULE

You can change the Firewall action that is applied to all application network rules that were created by default, and change the Firewall action that is applied to a single custom application network rule.

➤ *To change the Firewall response for all application network rules:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.

3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. To change the Firewall action for all network rules that are created by default, in the list of applications, select an application.

Custom application network rules are left unchanged.

5. In the **Network** column, click to display the context menu and select the action that you want to assign:

- **Inherit**
- **Allow**
- **Block**

6. In the **Firewall** window, click **OK**.

7. To save changes, click the **Save** button.

➡ *To modify the Firewall response for an application network rule:*

1. Open the application settings window (on page [48](#)).

2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

The settings of the Firewall and Network Attack Blocker components are shown in the right part of the window.

3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. In the list of applications, select the desired application.

5. Right-click to bring up the context menu and select **Application rules**.

The **Application control rules** window opens.

6. In the **Application control rules** window that opens, select the **Network rules** tab.

7. In the list of application network rules, select the network rule for which you want to change the Firewall action.

8. In the **Permission** column, right-click to bring up the context menu and select the action that you want to assign:

- **Allow**
- **Block**
- **Log events**

9. Click **OK**.

10. In the **Firewall** window, click **OK**.

11. To save changes, click the **Save** button.

CHANGING THE PRIORITY OF AN APPLICATION NETWORK RULE

The priority of an application network rule is determined by its position in the list of network rules. Firewall executes rules in the order in which they appear in the list of network rules, from top to bottom. According to each processed network rule that applies to a particular network connection, Firewall either allows or blocks network access to the address and port that are indicated in the settings of this network connection.

Custom application network rules have a higher priority than network rules that are inherited from the parent application group.

You cannot change the priority of inherited application network rules. Application network rules (both inherited ones and custom ones) hold priority over the application group network rules. In other words, all applications within a group automatically inherit the network rules for the group. However, when any rule is modified or created for a particular application, this rule is processed ahead of all of the inherited rules.

➤ *To change the priority of an application network rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Application network rules** button.

The **Firewall** window opens to the **Application control rules** tab.

4. In the list of applications, select the desired application.
5. Right-click to bring up the context menu and select **Application rules**.
The **Application control rules** window opens.
6. In the **Application control rules** window that opens, select the **Network rules** tab.
7. In the list of application network rules, select the application network rule whose priority you want to edit.
8. Use the **Up** and **Down** buttons to move the application network rule to the desired spot in the list of application network rules.
9. In the **Application control rules** window, click **OK**.
10. In the **Firewall** window, click **OK**.
11. To save changes, click the **Save** button.

CONFIGURING ADVANCED FIREWALL SETTINGS

You can configure advanced Firewall settings.

➤ *To configure advanced Firewall settings:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the settings of the Firewall component are displayed.
3. Click the **Network packet rules** button.

The **Firewall** window opens to the **Network packet rules** tab.

4. Click the **Additional** button.

The **Additional** window opens.

5. In the **Additional** window that opens, perform one of the following:
 - To enable a setting, select the check box next to the name of the advanced setting.
 - To disable a setting, clear the check box next to the name of the advanced setting.

Advanced Firewall settings include the following:

- **Allow active FTP mode.**
- **Block connections if there is no possibility to prompt for action (the application interface is not loaded).**
- **Do not disable Firewall until the operating system stops completely.**

Advanced Firewall settings are enabled by default.

6. In the **Additional** window, click **OK**.
7. To save changes, click the **Save** button.

NETWORK ATTACK BLOCKER

This section contains information about Network Attack Blocker and instructions on how to configure the component settings.

IN THIS SECTION:

About Network Attack Blocker.....	104
Enabling and disabling Network Attack Blocker	105
Editing the settings used in blocking an attacking computer	106

ABOUT NETWORK ATTACK BLOCKER

Network Attack Blocker scans inbound network traffic for activity that is typical of network attacks. On detecting an attempted network attack that targets your computer, Kaspersky Endpoint Security blocks network activity from the attacking computer. A warning then appears, which states that an attempted network attack has taken place and shows information about the attacking computer.

Network traffic from the attacking computer is blocked for one hour. You can edit the settings for blocking an attacking computer (see the section "Editing the settings used in blocking an attacking computer" on page [106](#)).

Descriptions of currently known types of network attacks and ways to fight them are provided in Kaspersky Endpoint Security databases. The list of network attacks that are detected by Network Attack Blocker is updated during database and application module updates (see the section "About database and application module updates" on page [159](#)).

ENABLING AND DISABLING NETWORK ATTACK BLOCKER

By default, Network Attack Blocker is enabled, functioning in the optimal mode. You can disable Network Attack Blocker, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))



➤ *To enable or disable Network Attack Blocker, do the following on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.



The **Protection** section opens.

4. Right-click the **Network Attack Blocker** line to display the context menu of Network Attack Blocker actions.
5. Do one of the following:

- To enable Network Attack Blocker, select **Enable** in the context menu.

The component status icon  that is displayed on the left in the **Network Attack Blocker** line changes to the icon .

- To disable Network Attack Blocker, select **Disable** in the context menu.

The component status icon  that is displayed on the left in the **Network Attack Blocker** line changes to the icon .

➤ *To enable or disable Network Attack Blocker in the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, under **Anti-Virus protection**, select **Network Attack Blocker**.

The Network Attack Blocker settings are displayed in the right part of the window.

3. Do the following:
 - To enable Network Attack Blocker, select the **Enable Network Attack Blocker** check box.
 - To disable Network Attack Blocker, clear the **Enable Network Attack Blocker** check box.
4. To save changes, click the **Save** button.

EDITING THE SETTINGS USED IN BLOCKING AN ATTACKING COMPUTER

➔ To edit the settings for blocking an attacking computer:

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Network Attack Blocker** section.

The Network Attack Blocker settings are displayed in the right part of the window.

3. In the **Network Attack Blocker** section, select the **Add the attacking computer to the list of blocked computers for** check box.

If this check box is selected, on detecting a network attack attempt, Network Attack Blocker blocks network traffic from the attacking computer for the specified amount of time. This protects the computer automatically against possible future network attacks from the same address.

If this check box is cleared, on detecting a network attack attempt, Network Attack Blocker does not enable automatic protection against possible future network attacks from the same address.

4. Change the amount of time during which an attacking computer is blocked in the field next to the **Add the attacking computer to the list of blocked computers for** check box.
5. To save changes, click the **Save** button.

MONITORING NETWORK TRAFFIC

This section contains information about network traffic monitoring and instructions on how to configure the settings of monitored network ports.

IN THIS SECTION:

About network traffic monitoring.....	106
Configuring the settings of network traffic monitoring.....	107

ABOUT NETWORK TRAFFIC MONITORING

During the operation of Kaspersky Endpoint Security, such components as Mail Anti-Virus (see the section "Email protection. Mail Anti-Virus" on page [64](#)), Web Anti-Virus (see the section "Computer protection on the Internet. Web Anti-Virus" on page [73](#)) and IM Anti-Virus (see the section "Protection of instant messaging client traffic. IM Anti-Virus" on page [80](#)) monitor data streams that are transmitted via specific protocols and pass through open TCP and UDP ports on your computer. For example, Mail Anti-Virus scans data that is transmitted via SMTP, while Web Anti-Virus scans data that is transmitted via the HTTP, HTTPS, and FTP protocols.

Kaspersky Endpoint Security divides TCP and UDP ports of the operating system into several groups, depending on the likelihood of their being compromised. Some network ports are reserved for services that may be vulnerable. You are advised to monitor these ports more thoroughly, because the likelihood that they are attacked is greater. If you use non-standard services that rely on non-standard network ports, these network ports may also be targeted by an attacking computer. You can specify a list of network ports and a list of applications that request network access. These ports and applications then receive special attention from the Mail Anti-Virus, Web Anti-Virus, and IM Anti-Virus components as they monitor network traffic.

CONFIGURING THE SETTINGS OF NETWORK TRAFFIC MONITORING

You can perform the following actions to configure the settings of network traffic monitoring:

- Enable monitoring of all network ports.
- Create a list of monitored network ports.
- Create a list of applications for which all network ports are monitored.

IN THIS SECTION:

Enabling monitoring of all network ports	107
Creating a list of monitored network ports	107
Creating a list of applications for which all network ports are monitored	108

ENABLING MONITORING OF ALL NETWORK PORTS

➔ *To enable monitoring of all network ports:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Monitored ports** section, select **Monitor all network ports**.
4. To save changes, click the **Save** button.

CREATING A LIST OF MONITORED NETWORK PORTS

➔ *To create a list of monitored network ports:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus Protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Monitored ports** section, select **Monitor selected ports only**.
4. Click the **Settings** button.

The **Network ports** window opens. The **Network ports** window displays a list of network ports that are normally used for transmission of email and network traffic. This list of network ports is included in the Kaspersky Endpoint Security package.

5. In the list of network ports, perform the following:
 - Select the check boxes opposite those network ports that you want to include in the list of monitored network ports.

By default, the check boxes are selected opposite all network ports that are listed in the **Network ports** window.

- Clear the check boxes opposite those network ports that you want to exclude from the list of monitored network ports.
6. If a network port is not shown in the list of network ports, add it by doing the following:
 - a. Under the list of network ports, click the **Add** link to open the **Network port** window.
 - b. Enter the network port number in the **Port** field.
 - c. Enter the name of the network port in the **Description** field.
 - d. Click **OK**.

The **Network port** window closes. The newly added network port is shown at the end of the list of network ports.

7. In the **Network ports** window, click **OK**.
8. To save changes, click the **Save** button.

CREATING A LIST OF APPLICATIONS FOR WHICH ALL NETWORK PORTS ARE MONITORED

You can create a list of applications for which Kaspersky Endpoint Security monitors all network ports.

We recommend including applications that receive or transmit data via the FTP protocol in the list of applications for which Kaspersky Endpoint Security monitors all network ports.

➔ *To create a list of applications for which all network ports are monitored:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus Protection** section.

The anti-virus protection settings are shown in the right part of the window.
3. In the **Monitored ports** section, select **Monitor selected ports only**.
4. Click the **Settings** button.

The **Network ports** window opens.
5. Select the **Monitor all ports for selected applications** check box.

This check box is selected by default.
6. In the list of applications under the **Monitor all ports for selected applications** check box, do the following:
 - Select the check boxes next to the names of applications for which you want to monitor all network ports.

By default, the check boxes are selected next to all applications that are listed in the **Network ports** window.
 - Clear the check boxes next to the names of applications for which you do not want to monitor all network ports.
7. If an application is not included in the list of applications, add it as follows:
 - a. Click the **Add** link under the list of applications and open the context menu.

- b. In the context menu, select the way in which to add the application to the list of applications:
 - To select an application from the list of applications that are installed on the computer, select the **Applications** command. The **Select application** window opens, letting you specify the name of the application.
 - To specify the location of the application's executable file, select the **Browse** command. The standard **Open** window in Microsoft Windows opens, letting you specify the name of the application executable file.
 - c. The **Application** window opens after you select the application.
 - d. In the **Name** field, enter a name for the selected application.
 - e. Click **OK**.

The **Application** window closes. The application that you have added appears at the end of the list of applications.
8. In the **Network ports** window, click **OK**.
 9. To save changes, click the **Save** button.

NETWORK MONITOR

This section contains information about Network Monitor and instructions on how to start Network Monitor.

IN THIS SECTION:

About Network Monitor.....	110
Starting Network Monitor.....	110

ABOUT NETWORK MONITOR

Network Monitor is a tool designed for viewing information about network activity in real time.

STARTING NETWORK MONITOR

➔ *To start Network Monitor:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Protection** section.

The **Protection** section opens.

4. Right-click the **Network Protection** line to display the context menu of Firewall operations.
5. In the context menu, select **Network Monitor**.

The **Network Monitor** window opens. In this window, information about the network activity of the computer is shown on four tabs:

- The **Network Activity** tab shows all current network connections with the computer. Both outbound and inbound network connections are displayed.
- The **Open Ports** tab lists all open network ports of the computer.
- The **Network Traffic** tab shows the volume of inbound and outbound network traffic between the user's computer and other computers in the network to which the user is currently connected.
- The **Blocked Computers** tab lists the IP addresses of remote computers whose network activity has been blocked by the Network Attack Blocker component after detecting network attack attempts from such IP addresses.

APPLICATION STARTUP 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 that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

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

IN THIS SECTION:

About Application Startup Control	111
Enabling and disabling Application Startup Control.....	111
About Application Startup Control rules	113
Managing Application Startup Control rules	115
Editing Application Startup Control message templates.....	119
About Application Startup Control operation modes.....	120
Switching from Black List mode to White List mode	120

ABOUT APPLICATION STARTUP CONTROL

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

Startup of applications whose parameters do not match any of the Application Startup Control rules is regulated by the default "Allow all" rule. The "Allow all" rule allows any user to start any application.

All user attempts to start applications are recorded in reports (see the section "Managing reports" on page [193](#)).

ENABLING AND DISABLING APPLICATION STARTUP CONTROL

Although Application Startup Control is enabled by default, you can disable Application Startup Control if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➔ *To enable or disable Application Startup Control on the Protection and Control tab of the main application window:*

1. Open the main application window.

2. Select the **Protection and Control** tab.
3. Click the **Endpoint control** section.



The **Endpoint control** section opens.

4. Right-click to bring up the context menu of the line with information about the Application Startup Control component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable Application Startup Control, select **Enable** in the menu.

The component status icon , which is displayed on the left in the **Application Startup Control** line, changes to the icon .

- To disable the Application Startup Control component, select **Disable** in the menu.

The component status icon , which is displayed on the left in the **Application Startup Control** line, changes to the icon .

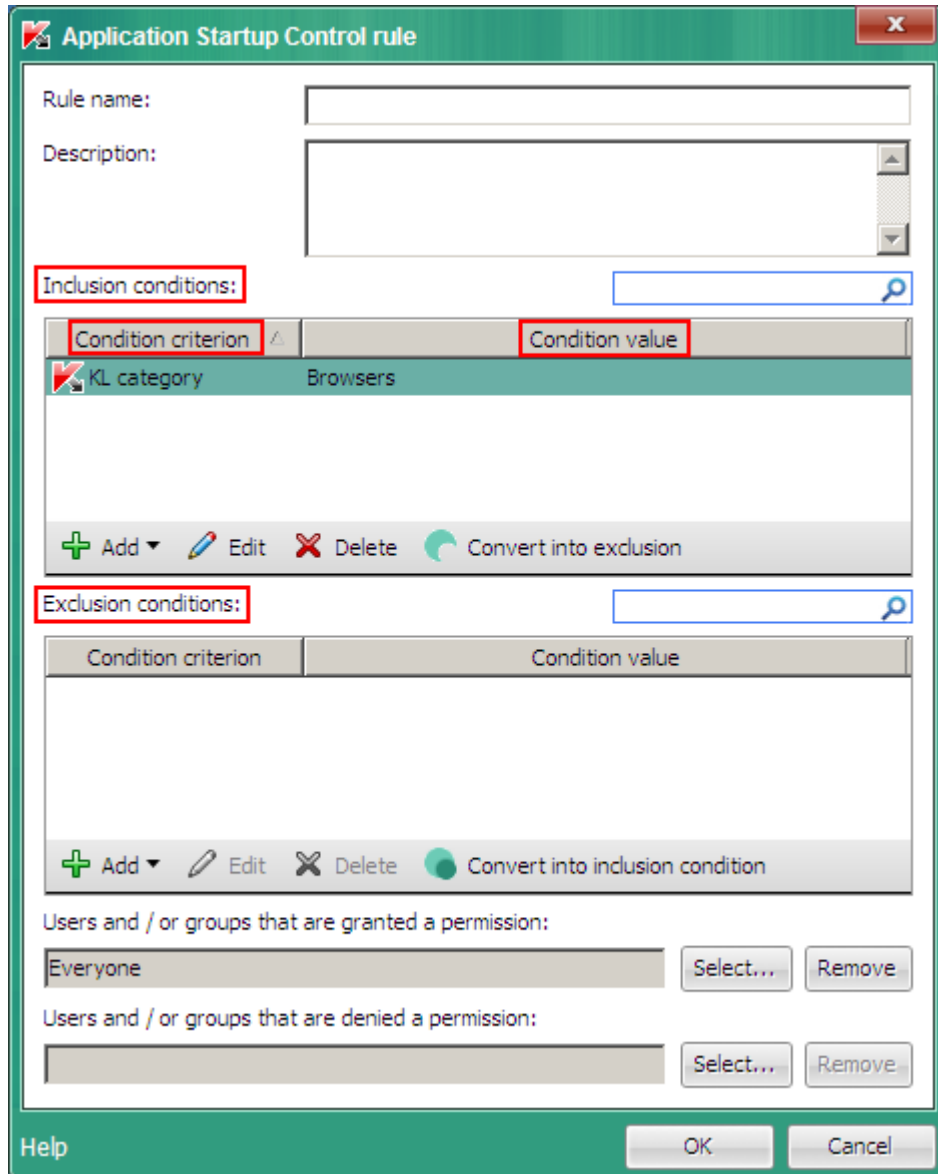
➡ *To enable or disable Application Startup Control from the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Startup Control**.
In the right part of the window, the settings of the Application Startup Control component are displayed.
3. Do one of the following:
 - To enable Application Startup Control, select the **Enable Application Startup Control** check box.
 - To disable Application Startup Control, clear the **Enable Application Startup Control** check box.
4. To save changes, click the **Save** button.

ABOUT APPLICATION STARTUP CONTROL RULES

An Application Startup Control rule is a group of settings that define the following functions of the Application Startup Control component:

- Classification of applications based on *rule-triggering conditions* (also called "conditions"). A rule-triggering condition represents the following correspondence: condition criterion – condition value – condition type (see the following figure).



Possible criteria of a rule-triggering condition:

- Path to the folder containing the executable file of the application or path to the executable file of the application.
- Metadata (the original name of the executable file of an application, the name of the executable file of an application on the drive, the version of the executable file of an application, the application name, and the application vendor)
- MD5 hash of the executable file of an application

- Inclusion of the application in a KL category. A KL category is a list of applications that have shared theme attributes. The list is maintained by Kaspersky Lab specialists.

For example, the KL category of "Office applications" includes all applications of the Microsoft Office suite, Adobe® Acrobat®, and others.

The type of rule-triggering condition determines the procedure by which an application is matched to a rule:

- *Inclusion conditions.* An application matches a rule if its parameters match at least one of the rule-triggering inclusion conditions.
- *Exclusion conditions.* An application does not match a rule if its parameters match at least one exclusion condition of a rule or do not match any inclusion conditions that trigger a rule. This rule does not control the start of such applications.
- Allowing selected users and / or user groups to start applications.

You can select a user and / or user group that is allowed to start applications that match an Application Startup Control rule.

A rule that does not specify any users who are allowed to start applications that match the rule is called a *block* rule.

- Blocking selected users and / or user groups from starting applications.

You can select a user and / or user group that is blocked from starting applications that match an Application Startup Control rule.

A rule that does not specify any users who are blocked from starting applications that match the rule is called an *allow* rule.

The priority of a block rule is higher than the priority of an allow rule. For example, if an Application Startup Control allow rule has been configured for a user group while an Application Startup Control block rule has been configured for one user in this user group, this user will be blocked from running the application.

Status of Application Startup Control rules

Application Startup Control rules can have one of three status values:

- *On.* This rule status means that the rule is enabled.
- *Off.* This rule status means that the rule is disabled.
- *Test.* This rule status means that Kaspersky Endpoint Security does not restrict application startup according to the rule settings, but only logs information about application startup in reports (see the section "Managing reports" on page [193](#)).

The *Test* status of a rule is convenient for testing the operation of a configured Application Startup Control rule. The user is not blocked from starting applications that match a rule with the *Test* status. Application allow and block settings are configured separately for test rules and non-test rules. For example, if a user is subject to a test allow rule of Application Startup Control and a non-test block rule of Application Startup Control, then

Default Application Startup Control rules

The following Application Startup Control rules are created by default:

- **Allow all.** This rule allows all users to start all applications. This rule governs the operation of Application Startup Control in Black List mode (see the section "About Application Startup Control operation modes" on page [120](#)). The rule is enabled by default.

- **Trusted updaters.** The rule allows startup of applications that have been installed or updated by applications in the KL category "Trusted Updaters" and for which no block rules have been configured. The "Trusted updaters" KL category includes updaters for the most reputable software vendors. This rule is created by default only on the on the Plugin Manager side of Kaspersky Endpoint Security. The rule is disabled by default.
- **Operating system and its components.** This rule allows all users to start applications in the "Golden Image" KL category. The "Golden Image" KL category includes applications that are required for the operating system to start and function normally. Permission to run applications belonging to this KL category is required for the operation of Application Startup Control in White List mode" (see the section "About Application Startup Control operation modes" on page [120](#)). This rule is created by default only on the on the Plugin Manager side of Kaspersky Endpoint Security. The rule is disabled by default.

MANAGING APPLICATION STARTUP CONTROL RULES

You can manage an Application Startup Control rule as follows:

- Add a new rule.
- Edit a rule.
- Edit rule status.

An Application Startup Control rule can be enabled (*On* status), disabled (*Off* status), or work in test mode (*Test* status). When created, an Application Startup Control rule is enabled by default (the rule has *On* status). You can disable an Application Startup Control rule or enable it in test mode.

- Delete a rule.

IN THIS SECTION:

Adding and editing an Application Startup Control rule	115
Adding a trigger condition for an Application Startup Control rule	116
Editing the status of an Application Startup Control rule	118

ADDING AND EDITING AN APPLICATION STARTUP CONTROL RULE

➡ *To add or edit an Application Startup Control rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Startup Control**.

In the right part of the window, the settings of the Application Startup Control component are displayed.
3. Do one of the following:
 - To add a rule, click the **Add** button.
 - To edit a rule, click the **Edit** button.

The **Application Startup Control rule** window opens.

4. Specify or edit the settings of the rule. To do so:
 - a. In the **Name** field, enter or edit the name of the rule.

- b. In the **Inclusion conditions** table, create (see page [116](#)) or edit the list of inclusion conditions that trigger an application startup control rule. To do so, use the **Add**, **Edit**, **Remove**, and **Convert into exclusion** buttons.
 - c. In the **Exclusion conditions** table, create or edit the list of exclusion conditions that trigger an Application Startup Control rule. To do so, use the **Add**, **Edit**, **Remove**, and **Convert into inclusion** buttons.
 - d. You can change the type of rule trigger condition. To do so:
 - To change the condition type from an inclusion condition to an exclusion condition, select a condition in the **Inclusion conditions** table and click the **Convert into exclusion** button.
 - To change the condition type from an exclusion condition to an inclusion condition, select a condition in the **Exclusion conditions** table and click the **Convert into inclusion** button.
 - e. Compile or edit a list of users and / or groups of users who are allowed to start applications that meet the rule inclusion conditions. To do so, enter the names of users and / or user groups manually in the **Users and / or groups that are granted a permission** field or click the **Select** button. The standard **Select Users or Groups** window in Microsoft Windows opens. This window lets you select users and / or user groups.
 - f. Compile or edit a list of users and / or groups of users who are blocked from starting applications that meet the rule inclusion conditions. To do so, enter the names of users and / or user groups manually in the **Users and / or groups that are denied a permission** field or click the **Select** button. The standard **Select Users or Groups** window in Microsoft Windows opens. This window lets you select users and / or user groups.
5. Click **OK**.
 6. To save changes, click the **Save** button.

ADDING A TRIGGER CONDITION FOR AN APPLICATION STARTUP CONTROL RULE

➔ *To add a condition for an Application Startup Control rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Startup Control**.
In the right part of the window, the settings of the Application Startup Control component are displayed.
3. Do one of the following:
 - To add a condition that triggers a new Application Startup Control rule, click the **Add** button.
 - To add a trigger condition to an existing Application Startup Control rule, select the relevant rule in the **Application Startup Control rules** list and click the **Add** button.

The **Application Startup Control rule** window opens.

4. In the **Inclusion conditions** or **Exclusion conditions** tables with conditions that trigger Application Startup Control rules, click the **Add** button.

The context menu of the **Add** button opens.

5. Do the following:

- To use file properties as the basis for a condition that triggers an Application Startup Control rule, select **Condition from properties of file**. To do so:

- a. In the standard **Open** window of Microsoft Windows, select an executable file whose properties you want to use as the basis for a condition that triggers an Application Startup Control rule.
- b. Click the **Open** button.

The **Condition from properties of file** window opens. The settings in the **Condition from properties of file** window have values that are extracted from the properties of the selected executable application file.

- c. In the **Condition from properties of file** window, select the criterion based on which you want to create one or more conditions that trigger the rule: **Metadata**, **Path to file or folder**, **File hash code (MD5)**, or the **KL category** to which the executable file of the application belongs. To do so, select the corresponding setting.
- d. Edit the settings of the selected condition criterion, if necessary.
- e. Click **OK**.

- To create one or several conditions that trigger an Application Startup Control rule on the basis of properties of files in a specified folder, select **Condition(s) from properties of files in the specified folder**. To do so:

- a. In the **Select folder** window, select a folder that contains executable application files whose properties you want to use as the basis for one or several conditions for triggering an Application Startup Control rule.
- b. Click **OK**.

The **Add condition** window opens.

- c. In the **Folder** field, edit the path to the folder with the executable application files, if necessary. To do so, click the **Select** button. The **Select folder** window opens. You can select the relevant folder in this window.
- d. In the **Add by criterion** drop-down list that opens, select the criterion based on which you want to create one or several conditions for triggering the rule: **Metadata**, **Folder path**, **File hash code (MD5)**, or **KL category** to which the executable application file belongs.

If your selection in the **Add by criterion** drop-down list is **Metadata**, select the check boxes opposite the executable file properties that you want to use in the condition that triggers the rule: **Original file name**, **File name on drive**, **File version**, **Application name**, **Application version**, and **Vendor**.

- e. Select the check boxes opposite the names of executable files whose properties you want to include in the condition(s) for triggering the rule.
- f. Click the **Next** button.

A list of formulated rule trigger conditions appears.

- g. In the list of formulated rule trigger conditions, select check boxes opposite rule trigger conditions that you want to add to the Application Startup Control rule.
- h. Click the **Finish** button.

- To create one or several conditions that trigger Application Startup Control rules on the basis of the properties of applications that are running in the operating system, select **Condition(s) from properties of started applications**. To do so:
 - a. In the **Add condition** window, open the **Add by criterion** drop-down list and select the criterion based on which you want to create one or several conditions triggering the rule: **Metadata**, **Folder path**, **File hash code (MD5)**, or **KL category** to which the executable application file belongs.

If your selection in the **Add by criterion** drop-down list is **Metadata**, select the check boxes opposite the executable file properties that you want to use in the condition that triggers the rule: **Original file name**, **File name on drive**, **File version**, **Application name**, **Application version**, and **Vendor**.
 - b. Select the check boxes opposite the names of executable files whose properties you want to include in the condition(s) for triggering the rule.
 - c. Click the **Next** button.

A list of formulated rule trigger conditions appears.
 - d. In the list of formulated rule trigger conditions, select check boxes opposite rule trigger conditions that you want to add to the Application Startup Control rule.
 - e. Click the **Finish** button.
- To create one or several conditions that trigger an Application Startup Control rule on the basis of the KL category criterion, select **Condition(s) "KL category"**. To do so:
 - a. In the **Condition(s) "KL category"** window, select check boxes opposite the names of those KL categories based on which you want to create the conditions that trigger the rule.
 - b. Click **OK**.
- To manually create a condition of triggering an Application Startup Control rule, select **Custom condition**. To do so:
 - a. In the **Custom condition** window, type the path to the executable application file. To do so, click the **Select** button. The **Open** window in Microsoft Windows opens. This window lets you select the executable application file.
 - b. Select the criterion based on which you want to create one or more conditions that trigger the rule: **Metadata**, **File or folder path**, **File hash code (MD5)**, or the **KL category** to which the executable file of the application belongs. To do so, select the corresponding setting.
 - c. Edit the settings of the selected condition criterion, if necessary.
 - d. Click **OK**.
- To create a condition for triggering an Application Startup Control rule based on the details of the drive that stores the executable application file, select **Condition by file drive**. To do so:
 - a. In the **Condition by file drive** window, open the **Drive** drop-down list to select the type of drive from which the start of applications is controlled by the Application Startup Control rule.
 - b. Click **OK**.

EDITING THE STATUS OF AN APPLICATION STARTUP CONTROL RULE

- *To edit the status of an Application Startup Control rule:*
 1. Open the application settings window (on page [48](#)).
 2. In the left part of the window, in the **Endpoint control** section, select **Application Startup Control**.

In the right part of the window, the settings of the Application Startup Control component are displayed.

3. Select the rule whose status you want to edit.
4. In the **Status** column, do the following:
 - If you want to enable the use of the rule, select the *On* value.
 - If you want to disable the use of the rule, select the *Off* value.
 - If you want the rule to work in test mode, select the *Test* value.
5. To save changes, click the **Save** button.

EDITING APPLICATION STARTUP CONTROL MESSAGE TEMPLATES

When a user attempts to start an application that is blocked by an Application Startup Control rule, Kaspersky Endpoint Security displays a message that the application is blocked from starting. If the user believes that the application is blocked from starting by mistake, the user can use the link in the message text to send a complaint to the LAN administrator.

Special templates are available for the block message and the complaint message. You can modify the message templates.

► To edit a message template:

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Startup Control**.
In the right part of the window, the settings of the Application Startup Control component are displayed.
3. In the right part of the window, click the **Templates** button.
The **Templates** window opens.
4. Do one of the following:
 - To edit the template of the message that is displayed when an application is blocked from starting, select the **Blockage** tab.
 - To modify the template of the complaint message that is sent to the LAN administrator, select the **Complaint** tab.
5. Modify the template of the blocking message or the complaint message. To do this, use the **By default** and **Variables** buttons.
6. Click **OK**.
7. To save changes, click the **Save** button.

ABOUT APPLICATION STARTUP CONTROL OPERATION MODES

The Application Startup Control component works in two modes:

- **Black list.** In this mode, Application Startup Control allows all users to start all applications, except for applications that are specified in block rules of Application Startup Control (see the section "About Application Startup Control rules" on page [113](#)).

This mode of Application Startup Control is enabled by default. Permission to start all applications is based on the default "Allow all" rule of Application Startup Control.

- **White list.** In this mode, Application Startup Control blocks all users from starting any applications, except for applications that are specified in allow rules of Application Startup Control. When the allow rules of Application Startup Control are fully configured, Application Startup Control blocks all new applications that have not been verified by the LAN administrator from starting, while allowing the operation of the operating system and of trusted applications that users rely on in their work.

Application Startup Control can be configured to operate in these modes both by using the Kaspersky Endpoint Security local interface and on the Kaspersky Security Center side.

However, Kaspersky Security Center offers tools that are not available in the Kaspersky Endpoint Security local interface, such as the tools that are needed to:

- Create application categories (see the section "Stage 2. Creating application categories" on page [121](#)). Application Startup Control rules on the Kaspersky Security Center side are based on custom application categories, and not on inclusion and exclusion rules as is the case in the Kaspersky Endpoint Security local interface.
- Gather information about applications that are installed on LAN computers (see the section "Stage 1. Gathering information about applications that are installed on LAN computers" on page [121](#)).
- Analyze the performance of Application Startup Control after a mode change (see the section "Stage 4. Testing allow rules of Application Startup Control" on page [123](#)).

This is why it is recommended to configure the Application Startup Control component on the side of Kaspersky Security Center.

SWITCHING FROM BLACK LIST MODE TO WHITE LIST MODE

This section describes how you can switch Application Startup Control from Black List mode to White List mode on the Kaspersky Security Center side, and also contains recommendations on how to make the most of Application Startup Control functionality.

IN THIS SECTION:

Stage 1. Gathering information about applications that are installed on user computers	121
Stage 2. Creating application categories.....	121
Stage 3. Creating allow rules of Application Startup Control.....	122
Stage 4. Testing allow rules of Application Startup Control.....	123
Stage 5. Switching to White List mode.....	123
Changing the status of an Application Startup Control rule on the Kaspersky Security Center side	124

STAGE 1. GATHERING INFORMATION ABOUT APPLICATIONS THAT ARE INSTALLED ON USER COMPUTERS

This stage involves getting a picture of the applications that are used on computers on the local area network. It is recommended to gather information about:

- Versions of Microsoft Windows operating systems
- Executable files that are started at operating system startup Which of these executable files belong to the operating system and which are essential to business processes
- Vendors whose applications are trusted on the local area network
- Office applications and their versions
- Specialized in-house software
- Standard corporate application suites and their contents
- Storages of setup files on the local area network

Information about applications that are used on computers on the local area network is available in the **Applications registry** folder and in the **Executable files** folder. The **Applications registry** folder and the **Executable files** folder are located in the **Applications and vulnerabilities** folder in the Kaspersky Security Center console tree.

The **Applications registry** folder contains the list of applications that were detected by the Network Agent which is installed on the client computers.

The **Executable files** folder contains a list of executable files that have ever been started on client computers or have been detected during the inventory task of Kaspersky Endpoint Security (see the section "About tasks for Kaspersky Endpoint Security" on page [228](#)).

To view general information about the application and its executable files, and the list of computers on which an application is installed, open the properties window of an application that is selected in the **Applications registry** folder or in the **Executable files** folder.

STAGE 2. CREATING APPLICATION CATEGORIES

This stage involves creating application categories. Application Startup Control rules can be created on the basis of such categories.

It is recommended to create a "Work applications" category that covers the standard set of applications that are used at the company. If different user groups use different sets of applications in their work, a separate application category can be created for each user group.

➤ *To create an application category:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, open the **Administered computers** folder.
3. To open the context menu, right-click in the results pane.
4. In the context menu, select **New** → **Category**.

The Application Category Creation Wizard opens.

5. Follow the instructions of the Application Category Creation Wizard.

STAGE 3. CREATING ALLOW RULES OF APPLICATION STARTUP CONTROL

This stage involves creating Application Startup Control rules that allow local area network users to start applications from the categories that were created during the previous stage.

➤ *To create an allow rule of Application Startup Control:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the results pane, select the **Policies** tab.
4. Right-click to open the context menu of the policy.
5. In the context menu of the policy, select **Properties**.

The policy properties window opens.

6. In the policy properties window, select the **Application Startup Control** section.

In the right part of the window, the settings of the Application Startup Control component are displayed.

7. Click the **Add** button.

The **Application Startup Control rule** window opens.

8. In the **Category** dropdown list, select an application category that was created during the previous stage, and based on which you want to create an allow rule.
9. Specify the list of users and / or user groups that are allowed to start applications from the selected category. To do so, enter the names of users and / or user groups manually in the **Users and / or user groups granted permission** field or click the **Select** button. The standard **Select Users or Groups** window in Microsoft Windows opens. This window lets you select users and / or user groups.
10. Leave blank the list of users who are blocked from starting applications that belong to the selected category.
11. If you want Kaspersky Endpoint Security to consider applications from the category that is specified in the rule as trusted updaters, and to allow them to start other applications for which no Application Startup Control rules are defined, select the **Trusted updaters** check box.

12. Click **OK**.
13. In the **Application Startup Control** section of the policy properties window, click the **Apply** button.

STAGE 4. TESTING ALLOW RULES OF APPLICATION STARTUP CONTROL

This stage involves performing the following operations:

1. Change the status of created allow rules of Application Startup Control (see the section "Changing the status of an Application Startup Control rule on the Kaspersky Security Center side" on page [124](#)) to *Test*.
2. Analyze the operation of allow rules of Application Startup Control in test mode.

Analyzing the operation of Application Startup Control rules in test mode involves reviewing the Application Startup Control events that are reported to Kaspersky Security Center. The rules have been created correctly if all applications that you had in mind when creating the application category are allowed to start. Otherwise, we recommend revising the settings of your application categories and Application Startup Control rules.

➔ *To view Application Startup Control events in the Kaspersky Security Center event storage:*

1. Open the Administration Console of Kaspersky Security Center.
2. To view events involving allowed / blocked launches of applications, open the folder **Event selections \ Events \ Information events / Critical events** in the console tree.

The Kaspersky Security Center workspace to the right of the console tree shows a list of all events that match the selected importance level, and which were reported to Kaspersky Security Center during the period that is specified in the Administration Server properties.

3. To view event information, open the event properties in one of the following ways:
 - Double-click an event.
 - Right-click to display the context menu of the event and select **Properties**.
 - On the right of the list of events, click the **Open event properties** button.

STAGE 5. SWITCHING TO WHITE LIST MODE

This stage involves performing the following operations:

- Enable the Application Startup Control rules that have been created. This is done by changing the rule status from *Test* to *On*.
- Enable the "Trusted updaters" and "Operating system and its components" rules created by default. This is done by changing the rule status from *Off* to *On*.
- Disable the "Allow all" default rule. This is done by changing the rule status from *On* to *Off*.

SEE ALSO:

About Application Startup Control rules	113
Changing the status of an Application Startup Control rule on the Kaspersky Security Center side	124

CHANGING THE STATUS OF AN APPLICATION STARTUP CONTROL RULE ON THE KASPERSKY SECURITY CENTER SIDE

➔ *To edit the status of an Application Startup Control rule:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computers belong.
3. In the results pane, select the **Policies** tab.
4. Right-click to open the context menu of the policy.
5. In the context menu of the policy, select **Properties**.
The policy properties window opens.
6. In the policy properties window, select the **Application Startup Control** section.
In the right part of the window, the settings of the Application Startup Control component are displayed.
7. Select an Application Startup Control rule whose status you want to change.
8. In the **Status** column, do one of the following:
 - If you want to enable the use of the rule, select the *On* value.
 - If you want to disable the use of the rule, select the *Off* value.
 - If you want the rule to work in test mode, select the *Test* value.
9. Click the **Apply** button.

APPLICATION PRIVILEGE CONTROL

This component is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This component is not available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

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

IN THIS SECTION:

About Application Privilege Control	125
Enabling and disabling Application Privilege Control	126
Placing applications into groups	127
Modifying a trust group	128
Working with application control rules	129
Protecting operating system resources and identity data	134

ABOUT APPLICATION PRIVILEGE CONTROL

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

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

The Firewall component monitors the network activity of applications (see page [84](#)).

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

We recommend that you participate in Kaspersky Security Network to improve the performance of Application Privilege Control (see the section "Participating in Kaspersky Security Network" on page [237](#)). Data that is obtained through Kaspersky Security Network allows you to sort applications into groups with more accuracy and to apply optimum application control rules.

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

ENABLING AND DISABLING APPLICATION PRIVILEGE CONTROL

By default, Application Privilege Control is enabled, running in a mode that is recommended by Kaspersky Lab experts. You can disable Application Privilege Control, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➤ *To enable or disable Application Privilege Control on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Endpoint control** section.



The **Endpoint control** section opens.

4. Right-click to display the context menu of the line with information about the Application Privilege Control component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable Application Privilege Control, select **Enable**.

The component status icon , which is displayed on the left in the **Application Privilege Control** line, changes to the icon .

- To disable the Application Privilege Control component, select **Disable**.

The component status icon , which is displayed on the left in the **Application Privilege Control** line, changes to the icon .

➤ *To enable or disable Application Privilege Control from the application settings window:*

1. Open the application settings window.
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. In the right part of the window, do one of the following:
 - To enable Application Privilege Control, select the **Enable Application Privilege Control** check box.
 - To disable Application Privilege Control, clear the **Enable Application Privilege Control** check box.
4. To save changes, click the **Save** button.

PLACING APPLICATIONS INTO GROUPS

When an application is started for the first time, the Application Privilege Control component checks the security of the application and places the application in a trust group.

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 danger that the applications pose to the operating system.

The trust groups are as follows:

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

No operations are prohibited for these applications.

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

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

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

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

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

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

At the first stage of the application scan, Kaspersky Endpoint Security searches the internal database of known applications for a matching entry, and then sends a request to the Kaspersky Security Network database (see the section "Participating in Kaspersky Security Network" on page [237](#)) (if an Internet connection is available). If the application

matches an entry in the Kaspersky Security Network database, the application is assigned to the trust group that is specified in the Kaspersky Security Network database.

By default, Kaspersky Endpoint Security uses heuristic analysis to assign unknown applications to trust groups. During heuristic analysis, Kaspersky Endpoint Security identifies the threat level of an application. Kaspersky Endpoint Security assigns the application to a particular trust group based on its threat level. Instead of using heuristic analysis, you can specify a trust group to which Kaspersky Endpoint Security automatically assigns all unknown applications.

By default, Kaspersky Endpoint Security scans an application for 30 seconds. If the threat level of the application is not determined after this time expires, Kaspersky Endpoint Security places the application in the Low Restricted group and continues in background mode to attempt to determine the threat level of the application. After completing this process, Kaspersky Endpoint Security assigns the application to its final trust group. You can change the amount of time that is allocated for determining the threat level of applications that are started. If you are certain that all applications that are launched on the user's computer do not pose a threat to security, you can reduce the amount of time that is allocated for determining the threat level. If you install applications whose safety is questionable, you are advised to increase the amount of time that is allocated for determining the threat level.

If an application has a high threat level, Kaspersky Endpoint Security notifies the user, prompting the user to choose a trust group to which this application is to be assigned. This notification contains statistics about use of the application by Kaspersky Security Network participants. Based on these statistics and knowing how the application appeared on your computer, you can make an objective choice on which trust group to place the application in.

➤ *To configure the settings for placement of applications in trust groups:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.

In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. If you want to automatically place digitally signed applications in the Trusted group, select the **Trust digitally signed applications** check box.
4. Choose the way in which unknown applications are to be assigned to trust groups:
 - If you want to use heuristic analysis for assigning unknown applications to trust groups, select the option **Use heuristic analysis to determine group**.
 - If you want to assign all unknown applications to a specified trust group, select the option **Automatically move to group** and select the appropriate trust group in the drop-down list.
5. In the **Maximum time to determine group** field, specify the amount of time that is allotted for scanning started applications.
6. To save changes, click the **Save** button.

MODIFYING A TRUST GROUP

When an application is first started, Kaspersky Endpoint Security automatically places the application in a trust group. You can move the application to another trust group manually, if necessary.

Kaspersky Lab specialists do not recommend moving applications from the automatically assigned trust group to a different trust group. Instead, if required, edit the rules for an individual application (see the section "Editing application rules" on page [130](#)).

➤ *To change the trust group to which an application has been automatically assigned by Kaspersky Endpoint Security when first started:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.

In the right part of the window, the settings of the Application Privilege Control component are displayed.

3. Click the **Applications** button.

The **Application control rules** tab in the **Applications** window opens.

4. Select the relevant application on the **Application control rules** tab.
5. Do one of the following:
 - Right-click to display the context menu of the application. From the context menu of the application, select **Move to group** → □<group name>.
 - To open the context menu, click the **Trusted / Low Restricted / High Restricted / Untrusted** link. In the context menu, select the required trust group.
6. Click **OK**.
7. To save changes, click the **Save** button.

MANAGING 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.

IN THIS SECTION:

Editing control rules for trust groups and application groups.....	129
Editing an application control rule	130
Downloading and updating application control rules from the Kaspersky Security Network database.....	131
Disabling the inheritance of restrictions from the parent process.....	132
Excluding specific application actions from application control rules.....	133
Configuring storage settings for control rules that govern unused applications.....	133

EDITING CONTROL RULES FOR TRUST GROUPS AND APPLICATION GROUPS

The optimal application control rules for different trust groups are created by default. The settings of rules for application group control inherit values from the settings of trust group control rules. You can edit the preset trust group control rules and the rules for application group control.

➤ *To edit the trust group control rules or the rules for application group control:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.

3. Click the **Applications** button.

The **Application control rules** tab in the **Applications** window opens.

4. Select the relevant trust group or application group on the **Application control rules** tab.
5. Right-click to open the context menu of a trust group or of a group of applications.
6. From the context menu of a trust group or of a group of applications, select **Group rules**.

The **Application group control rules** window opens.

7. In the **Application group control rules** window, do one of the following:
 - To edit trust group control rules or rules for application group control that govern the rights of the trust group or application group to access the operating system registry, user files, and application settings, select the **Files and system registry** tab.
 - To edit trust group control rules or rules for application group control that govern the rights of the trust group or application group to access operating system processes and objects, select the **Rights** tab.
8. For the required resource, in the column of the corresponding action, right-click to open the context menu.
9. From the context menu, select the required item.
 - **Inherit**
 - **Allow**
 - **Block**
 - **Log events**

If you are editing trust group control rules, the **Inherit** item is not available.

10. Click **OK**.
11. In the **Applications** window, click **OK**.
12. To save changes, click the **Save** button.

EDITING AN APPLICATION CONTROL RULE

By default, the settings of application control rules of applications that belong to an application group or trust group inherit the values of settings of trust group control rules. You can edit the settings of application control rules.

➤ *To change an application control rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.

In the right part of the window, the settings of the Application Privilege Control component are displayed.

3. Click the **Applications** button.

The **Application control rules** tab in the **Applications** window opens.

4. Select the relevant application on the **Application control rules** tab.
5. Do one of the following:
 - Right-click to display the context menu of the application. From the context menu of the application, select **Group rules**.
 - Click the **Additional** button in the lower-right corner of the **Application control rules** tab.

The **Application control rules** window opens.

6. In the **Application control rules** window, do one of the following:
 - To edit application control rules that govern the rights of the application to access the operating system registry, user files, and application settings, select the **Files and system registry** tab.
 - To edit application control rules that govern the rights of the application to access operating system processes and objects, select the **Rights** tab.
7. For the required resource, in the column of the corresponding action, right-click to open the context menu.
8. From the context menu, select the required item.
 - **Inherit**
 - **Allow**
 - **Block**
 - **Log events**
9. Click **OK**.
10. In the **Applications** window, click **OK**.
11. To save changes, click the **Save** button.

DOWNLOADING AND UPDATING APPLICATION CONTROL RULES FROM THE KASPERSKY SECURITY NETWORK DATABASE

By default, applications that are in the Kaspersky Security Network database are processed according to the application control rules that are loaded from this database.

If an application was not in the Kaspersky Security Network database when started for the first time, but information about it was added to the database later, by default Kaspersky Endpoint Security automatically updates the control rules for this application.

You can disable downloads of application control rules from the Kaspersky Security Network database and automatic updates of control rules for previously unknown applications.

➤ *To disable downloads and updates of application control rules from the Kaspersky Security Network database:*

1. Open the application settings window (on page [48](#)).

2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. Clear the **Update control rules for previously unknown applications from KSN database** check box.
4. To save changes, click the **Save** button.

DISABLING THE INHERITANCE OF RESTRICTIONS FROM THE PARENT PROCESS

Application startup may be initiated either by the user or by another running application. When application startup is initiated by another application, a startup sequence is created, which consists of parent and child processes.

When an application attempts to obtain access to a protected resource, Application Privilege Control analyzes all parent processes of the application to determine whether these processes have rights to access the protected resource. The minimum priority rule is then observed: when comparing the access rights of the application to those of the parent process, the access rights with a minimum priority are applied to the application's activity.

The priority of access rights is as follows:

1. **Allow** This access right has the highest priority.
2. **Block** This access right has the lowest priority.

This mechanism prevents a non-trusted application or an application with restricted rights from using a trusted application to perform actions that require certain privileges.

If the activity of an application is blocked because a parent process has insufficient rights, you can edit these rights (see the section "Editing application control rules" on page [130](#)) or disable inheritance of restrictions from the parent process.

➡ *To disable the inheritance of restrictions from the parent process:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. Click the **Applications** button.
The **Application control rules** tab in the **Applications** window opens.
4. Select the relevant application on the **Application control rules** tab.
5. Right-click to display the context menu of the application.

6. From the context menu of the application, select **Group rules**.
The **Application control rules** window opens.
7. In the **Application control rules** window that opens, select the **Exclusions** tab.
8. Select the **Do not inherit restrictions of the parent process (application)** check box.
9. Click **OK**.
10. In the **Applications** window, click **OK**.
11. To save changes, click the **Save** button.

EXCLUDING SPECIFIC APPLICATION ACTIONS FROM APPLICATION CONTROL RULES

➤ *To exclude specific application actions from application control rules:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. Click the **Applications** button.
The **Application control rules** tab in the **Applications** window opens.
4. Select the relevant application on the **Application control rules** tab.
5. Right-click to bring up the context menu of the application and select **Application rules**.
The **Application control rules** window opens.
6. In the **Application control rules** window that opens, select the **Exclusions** tab.
7. Select check boxes next to application actions that do not need to be monitored.
8. Click **OK**.
9. In the **Applications** window, click **OK**.
10. To save changes, click the **Save** button.

CONFIGURING STORAGE SETTINGS FOR CONTROL RULES THAT GOVERN UNUSED APPLICATIONS

By default, control rules for applications that have not been started in 60 days are deleted automatically. You can change the storage duration for control rules for unused applications or disable the automatic deletion of rules.

➤ *To configure the storage settings for control rules that govern unused applications:*

1. Open the application settings window (on page [48](#)).

2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. Do one of the following:
 - If you want Kaspersky Endpoint Security to delete control rules of unused applications, select the **Delete control rules of applications unused for more than** check box and specify the relevant number of days.
 - To disable the automatic deletion of control rules of unused applications, clear the **Delete control rules of applications unused for more than** check box.
4. To save changes, click the **Save** button.

PROTECTING OPERATING SYSTEM RESOURCES AND IDENTITY DATA

Application Privilege Control manages application rights to take actions on various categories of operating system resources and of identity data.

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

You can perform the following actions:

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

IN THIS SECTION:

Adding a category of protected resources.....	134
Adding a protected resource	135
Disabling resource protection.....	136

ADDING A CATEGORY OF PROTECTED RESOURCES

➤ *To add a new category of protected resources:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. Click the **Resources** button.
The **Protected resources** tab in the **Applications** window opens.
4. In the left part of the **Protected resources** tab, select a section or category of protected resources to which you want to add a new category of protected resources.

5. Click to open the context menu of the **Add** button.
6. In the context menu, select **Category**.

The **Category of protected resources** window opens.

7. In the **Category of protected resources** window that opens, enter a name for the new category of protected resources.
8. Click **OK**.
A new item appears in the list of categories of protected resources.
9. In the **Applications** window, click **OK**.
10. To save changes, click the **Save** button.

After you add a category of protected resources, you can edit or remove it by clicking the **Edit** or **Delete** buttons in the upper-left part of the **Protected resources** tab.

ADDING A PROTECTED RESOURCE

➔ *To add a protected resource:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.
In the right part of the window, the settings of the Application Privilege Control component are displayed.
3. Click the **Resources** button.
The **Protected resources** tab in the **Applications** window opens.
4. In the left part of the **Protected resources** tab, select a category of protected resources to which you want to add a new protected resource.
5. In the upper-left part of the **Protected resources** tab, click to open the context menu of the **Add** button.
6. In the context menu, select the type of resource that you want to add:
 - **File or folder.**
 - **Registry key.**
 The **Protected resource** window opens.
7. In the **Protected resource** window, enter the name of the protected resource in the **Name** field.
8. Click the **Browse** button.
9. In the window that opens, specify the necessary settings depending on the type of protected resource that you want to add. Click **OK**.
10. In the **Protected resource** window, click **OK**.
A new item appears in the list of protected resources of the selected category on the **Protected resources** tab.
11. Click **OK**.

12. To save changes, click the **Save** button.

After you add a protected resource, you can edit or remove it by clicking the **Edit** or **Delete** buttons in the upper-left part of the **Protected resources** tab.

DISABLING RESOURCE PROTECTION

➤ *To disable resource protection:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Application Privilege Control**.

In the right part of the window, the settings of the Application Privilege Control component are displayed.

3. In the right part of the window, click the **Resources** button.

The **Protected resources** tab in the **Applications** window opens.

4. Do one of the following:

- In the left part of the tab, in the list of protected resources, select the resource for which you want to disable protection and clear the check box next to its name.

- Click **Exclusions** and do the following:

- a. In the **Exclusions** window, click to open the context menu of the **Add** button.
- b. In the context menu, select the type of resource that you want to add to the list of exclusions from protection by the Application Privilege Control component: **File or folder** or **Registry key**.

The **Protected resource** window opens.

- c. In the **Protected resource** window, enter the name of the protected resource in the **Name** field.
- d. Click the **Browse** button.
- e. In the window that opens, specify the necessary settings depending on the type of protected resource that you want to add to the list of exclusions from protection by the Application Privilege Control component.
- f. Click **OK**.
- g. In the **Protected resource** window, click **OK**.

A new element appears in the list of resources that are excluded from protection by the Application Privilege Control component.

After adding a resource to the list of exclusions from protection by the Application Privilege Control component, you can edit or remove it by clicking the **Edit** or **Delete** buttons in the upper part of the **Exclusions** window.

- h. In the **Exclusions** window, click **OK**.
5. In the **Applications** window, click **OK**.
6. To save changes, click the **Save** button.

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 that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

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

IN THIS SECTION:

About Device Control	137
Enabling and disabling Device Control.....	138
About device and connection bus access rules.....	139
About trusted devices.....	139
Standard decisions on access to devices.....	139
Editing a device access rule.....	140
Editing a connection bus access rule.....	141
Actions with trusted devices	142
Editing templates of Device Control messages	144
Obtaining access to a blocked device	144
Creating a device access code	146

ABOUT DEVICE CONTROL

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

- Data storage devices (hard disk drives, removable media, tape drives, CDs/DVDs)
- Data transfer tools (modems, external network cards)
- Devices that are designed for converting data to hard copies (printers)
- Connection buses (also referred to as "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").

ENABLING AND DISABLING DEVICE CONTROL

By default, Device Control is enabled. You can disable Device Control, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➤ *To enable or disable Device Control on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Endpoint control** section.



The **Endpoint control** section opens.

4. Right-click to bring up the context menu of the line with information about the Device Control component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable Device Control, select **Enable** in the menu.

The component status icon , which is displayed on the left in the **Device Control** line, changes to the icon .

- To disable Device Control, select **Disable** in the menu.

The component status icon , which is displayed on the left in the **Device Control** line, changes to the icon .

➤ *To enable or disable Device Control from the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.
In the right part of the window, the settings of the Device Control component are displayed.
3. Do one of the following:
 - If you want to enable Device Control, select the **Enable Device Control** check box.
 - If you want to disable Device Control, clear the **Enable Device Control** check box.
4. To save changes, click the **Save** button.

ABOUT DEVICE AND CONNECTION BUS ACCESS RULES

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.

A connection bus access rule allows or blocks access to a connection bus.

Rules that allow access to buses are created by default for all connection buses that are present in the classification of the Device Control component.

You cannot create or delete device access rules or connection bus access rules; you can only edit them.

ABOUT TRUSTED DEVICES

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.

STANDARD DECISIONS ON ACCESS TO DEVICES

Kaspersky Endpoint Security makes a decision on whether to allow access to a device after the user connects the device to the computer.

Table 2. Standard decisions on access to devices

No.	INITIAL CONDITIONS	INTERIM STEPS TO TAKE UNTIL A DECISION ON ACCESS TO THE DEVICE IS MADE			DECISION ON ACCESS TO THE DEVICE
		CHECKING WHETHER THE DEVICE IS INCLUDED IN THE LIST OF TRUSTED DEVICES	TESTING ACCESS TO THE DEVICE BASED ON THE ACCESS RULE	TESTING ACCESS TO THE BUS BASED ON BUS ACCESS RULE	
1	The device is not present in the device classification of the Device Control component.	Not included in the list of trusted devices.	No access rule.	Not subject to scanning.	Access allowed.
2	The device is trusted.	Included in the list of trusted devices.	Not subject to scanning.	Not subject to scanning.	Access allowed.
3	Access to the device is allowed.	Not included in the list of trusted devices.	Access allowed.	Not subject to scanning.	Access allowed.
4	Access to the device depends on the bus.	Not included in the list of trusted devices.	Access depends on the bus.	Access allowed.	Access allowed.
5	Access to the device depends on the bus.	Not included in the list of trusted devices.	Access depends on the bus.	Access blocked.	Access blocked.
6	Access to the device is allowed. No bus access rule is found.	Not included in the list of trusted devices.	Access allowed.	No bus access rule.	Access allowed.
7	Access to the device is blocked.	Not included in the list of trusted devices.	Access blocked.	Not subject to scanning.	Access blocked.
8	No device access rule or bus access rule is found.	Not included in the list of trusted devices.	No access rule.	No bus access rule.	Access allowed.
9	There is no device access rule.	Not included in the list of trusted devices.	No access rule.	Access allowed.	Access allowed.
10	There is no device access rule.	Not included in the list of trusted devices.	No access rule.	Access blocked.	Access blocked.

You can edit the device access rule after you connect the device. If the device is connected and the access rule allows access to it, but you later edit the access rule and block access, Kaspersky Endpoint Security blocks access the next time that any file operation is requested from the device (viewing the folder tree, reading, writing). A device without a file system is blocked only the next time that the device is connected.

EDITING A DEVICE ACCESS RULE

➔ *To edit a device access rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the settings of the Device Control component are displayed.

3. In the right part of the window, select the **Device types** tab.

The **Device types** tab contains access rules for all devices that are included in the classification of the Device Control component.

4. Select the access rule that you want to edit.
5. Click the **Edit** button. This button is only available for device types which have a file system.

The **Configure device access rule** window opens.

By default, a device access rule grants all users full access to the specified type of devices at any time. In the **Users and / or groups of users** list, this access rule contains the **All** group. In the **Rights of the selected group of users by access schedules** table, this access rule contains the **Any time** interval of access to devices, with the rights to perform all kinds of operations with devices.

6. Edit the settings of the device access rule:
 - a. To edit the **Users and / or groups of users** list, use the **Add**, **Edit**, and **Delete** buttons.
 - b. To edit the list of access schedules to devices, use the **Create**, **Edit**, **Copy**, and **Delete** buttons in the **Rights of the selected group of users by access schedules** table.
 - c. Select a user and / or group of users from the **Users and / or groups of users** list.
 - d. In the **Rights of the selected group of users by access schedules** table, configure the schedule for access to devices for the selected user and / or group of users. To do this, select the check boxes next to the names of the access schedules for devices that you want to use in the device access rule that is to be edited.
 - e. For each device access schedule for the selected user and / or user group, specify the operations that are allowed when working with devices. To do this, in the **Rights of the selected group of users by access schedules** table, select the check boxes in the columns with the names of the required operations.
 - f. Repeat steps c–e for the remaining items in the **Users and / or user groups** list.
 - g. Click **OK**.

Editing the default settings of device access rules causes the setting for access to the device type to change to *Allowed with restrictions*.

7. To save changes, click the **Save** button.

EDITING A CONNECTION BUS ACCESS RULE

➤ *To edit a connection bus access rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the settings of the Device Control component are displayed.

3. Select the **Connection buses** tab.

The **Connection buses** tab displays the access rules for all connection buses that are classified in the Device Control component.

4. Select the bus connection rule that you want to edit.

5. Change the value of the access parameter:
 - To allow access to a connection bus, click the **Access** column to open the context menu and select **Allow**.
 - To block access to a connection bus, click the **Access** column to open the context menu and select **Block**.
6. To save changes, click the **Save** button.

ACTIONS WITH TRUSTED DEVICES

This section contains information about actions with trusted devices.

IN THIS SECTION:

Adding a device to the list of trusted devices	142
Editing the Users setting of a trusted device	143
Removing a device from the list of trusted devices	143

ADDING A DEVICE TO THE LIST OF TRUSTED DEVICES

By default, when a device is added to the list of trusted devices, access to the device is granted to all users (the Everyone group of users).

➤ *To add a device to the list of trusted devices:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the settings of the Device Control component are displayed.

In the right part of the window, select the **Trusted devices** tab.
3. Click the **Add** button.

The **Add trusted devices** window opens.
4. Select the check box next to the name of a device that you want to add to the list of trusted devices.

The list in the **Devices** column depends on the value that is selected in the **Display connected devices** drop-down list.
5. Click the **Select** button.

The **Select Users or Groups** window in Microsoft Windows opens.
6. In the **Select Users or Groups** window in Microsoft Windows, specify users and / or groups of users for which Kaspersky Endpoint Security recognizes the selected devices as trusted.

The names of users and / or groups of users that are specified in the **Select users and / or groups of users** window of Microsoft Windows are displayed in the **Allow to users and / or groups of users** field.

7. In the **Add trusted devices** window, click **OK**.

In the table, on the **Trusted devices** tab of the **Device Control** component settings window, a line appears and displays the parameters of the trusted device that has been added.

8. Repeat steps 4–7 for each device that you want to add to the list of trusted devices for the specified users and / or user groups.
9. To save changes, click the **Save** button.

EDITING THE USERS SETTING OF A TRUSTED DEVICE

By default, when a device is added to the list of trusted devices, access to the device is granted to all users (the Everyone group of users). You can edit the **Users** setting of a trusted device.

➔ *To edit the Users setting of a trusted device:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.
In the right part of the window, the settings of the Device Control component are displayed.
3. In the right part of the window, select the **Trusted devices** tab.
4. From the list of trusted devices, select the device whose parameters you want to change.
5. Click the **Edit** button.
The standard **Select Users or Groups** window in Microsoft Windows opens.
6. Edit the list of users and / or user groups for which the device is set as trusted.
7. Click **OK**.
8. To save changes, click the **Save** button.

REMOVING A DEVICE FROM THE LIST OF TRUSTED DEVICES

➔ *To remove a device from the list of trusted devices:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.
In the right part of the window, the settings of the Device Control component are displayed.
3. In the right part of the window, select the **Trusted devices** tab.
4. Select the device that you want to remove from the list of trusted devices.
5. Click the **Delete** button.
6. To save changes, click the **Save** button.

A decision on access to a device that you have removed from the list of trusted devices is made by Kaspersky Endpoint Security based on device access rules and connection bus access rules.

EDITING TEMPLATES OF DEVICE CONTROL MESSAGES

When the user attempts to access a blocked device, Kaspersky Endpoint Security displays a message that access to the device is blocked or that the operation with the device content is forbidden. If the user believes that access to the device is blocked (or that an operation with device content is forbidden) by mistake, the user can click the link in the message text to send a complaint to the LAN administrator.

Templates are available for messages about blocked access to devices or forbidden operations with device content, and for complaint messages. You can modify the message templates.

➤ *To edit the template for Device Control messages:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.
In the right part of the window, the settings of the Device Control component are displayed.

3. In the right part of the window, click the **Templates** button.

The **Templates** window opens.

4. Do one of the following:
 - To modify the template of the message about blocked access to a device or a forbidden operation with device content, select the **Blockage** tab.
 - To modify the template of the complaint message that is sent to the LAN administrator, select the **Complaint** tab.
5. Modify the template of the blocking message or the complaint message. To do this, use the **By default** and **Variables** buttons.
6. Click **OK**.
7. To save changes, click the **Save** button.

OBTAINING ACCESS TO A BLOCKED DEVICE

A user can obtain access to a blocked device. To do this, the user must send a request from the Device Control component settings window or click the link in the message that informs that the device is blocked.

The Kaspersky Endpoint Security functionality that grants temporary access to a device is available only when Kaspersky Endpoint Security operates under the Kaspersky Security Center policy and this functionality is enabled in the policy settings.

➤ *To obtain access to a blocked device from the Device Control component settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.
In the right part of the window, the settings of the Device Control component are displayed.

3. Click the **Request access** button.

The **Request access to device** window opens.

4. From the list of connected devices, select the one to which you want to obtain access.
5. Click the **Request access key** button.

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

6. In the **Access duration** field, specify the time interval for which you want to have access to the device.
7. Click the **Save** button.

The standard **Save access key** window of Microsoft Windows opens.

8. In the **Save access key** window in Microsoft Windows, select the folder in which you want to save a file with a device access key, and click the **Save** button.
9. Pass the device access key file to the LAN administrator.
10. Receive the device access code from the LAN administrator.
11. In the **Request access to device** window, click the **Activate access code** button.

The standard **Open access key** window in Microsoft Windows opens.

12. In the **Open access key** window in Microsoft Windows, select the device access key file that was received from the LAN administrator, and click the **Open** button.

The **Activate device access code** window opens and displays information about the provided access.

13. In the **Activate device access code** window, click **OK**.

➔ *To obtain access to a blocked device by clicking the link in the message that informs that the device is blocked:*

1. In the window with the message that informs that a device or connection bus is blocked, click the **Request access** link.

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

2. In the **Access duration** field, specify the time interval for which you want to have access to the device.
3. Click the **Save** button.

The standard **Save access key** window of Microsoft Windows opens.

4. In the **Save access key** window in Microsoft Windows, select the folder in which you want to save a file with a device access key, and click the **Save** button.
5. Pass the device access key file to the LAN administrator.
6. Receive the device access code from the LAN administrator.
7. In the **Request access to device** window, click the **Activate access code** button.

The standard **Open access key** window in Microsoft Windows opens.

8. In the **Open access key** window in Microsoft Windows, select the device access key file that was received from the LAN administrator, and click the **Open** button.

The **Activate device access code** window opens and displays information about the provided access.

9. In the **Activate device access code** window, click **OK**.

The time period for which access to the device is granted may differ from the amount of time that you requested. Access to the device is granted for the time period that the LAN administrator specifies when generating the device access code.

CREATING A DEVICE ACCESS CODE

To grant a user temporary access to a device, an access code is required. A device access code can be created on the Kaspersky Security Center side.

➔ *To create a device access code:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select the computer whose user needs to be granted temporary access to a device.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. In the context menu of the client computer, select **Properties**.
 - In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. Select the **Tasks** section.

A list of local tasks for managing Kaspersky Endpoint Security is displayed in the right part of the window.
7. In the list of local tasks, select the **Device Control** task.
8. Do one of the following:
 - Right-click to display the context menu of the task. In the context menu of the task, select **Properties**.
 - Click the **Properties** button.

The **Properties: Device Control** window opens.

9. In the **Properties: Device Control** window, select the **Settings** section.

In the right part of the window, the settings of the Device Control local task are displayed.
10. In the right part of the window, click the **Grant access** button.

The **Allow temporary access to device** window opens.
11. In the **Allow temporary access to device** window, click the **Browse** button.

A standard Microsoft Windows **Select access key** window opens.

12. In the **Select access key** window of Microsoft Windows, select the access key file that you have received from the user and click the **Open** button.

The **Allow temporary access to device** window shows information about the device to which the user has requested access.

13. Specify the value of the **Access duration** setting. This setting defines the length of time for which you grant the user access to the device.

The default value is equal to the one that is specified by the user when creating the access key.

14. Specify the value of the **Activation period** setting. This setting defines the period during which the user can activate access to the device by using the activation code.

15. Click the **Save access code** button.

A standard Microsoft Windows **Save access key** window opens.

16. Select the destination folder in which you want to save the file with the device access code.

17. Click the **Save** button.

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 that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

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

IN THIS SECTION:

About Web Control	148
Enabling and disabling Web Control	149
About web resource access rules	150
Actions with web resource access rules	150
Exporting and importing the list of web resource addresses	154
Editing masks for web resource addresses	155
Editing templates of Web Control messages	157

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 "Social networks" 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 web resource access rules (see the section "About web resource access rules" on page [150](#)) (also referred to as "rules").

ENABLING AND DISABLING WEB CONTROL

By default, Web Control is enabled. You can disable Web Control, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➡ *To enable or disable Web Control on the Protection and Control tab of the main application window:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Endpoint control** section.



The **Endpoint control** section opens.

4. Right-click to bring up the context menu of the line with information about the Web Control component.



A menu for selecting actions on the component opens.

5. Do one of the following:

- To enable Web Control, select **Start** in the menu.

The component status icon , which is displayed on the left in the **Web Control** line, changes to the icon .

- To disable Web Control, select **Stop** in the menu.

The component status icon , which is displayed on the left in the **Web Control** line, changes to the icon .

➡ *To enable or disable Web Control from the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the settings of the Web Control component are displayed.

3. Do one of the following:

- If you want to enable Web Control, select the **Enable Web Control** check box.
- If you want to disable Web Control, clear the **Enable Web Control** check box.

If Web Control is disabled, Kaspersky Endpoint Security does not control access to web resources.

4. To save changes, click the **Save** button.

ABOUT WEB RESOURCE ACCESS RULES

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

The following filters are available:

- **Filter by content.** Web Control categorizes web resources by content and data type. You can control user access to web resources with content and data types of certain categories. When the users visit web resources that belong to the selected content category and / or data type category, Kaspersky Endpoint Security performs the action that is specified in the rule.
- **Filter by web resource addresses.** You can control user access to all web resource addresses or to individual web resource addresses and / or groups of web resource addresses.

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

- **Filter by names of users and user groups.** You can specify the names of users and / or groups of users for which access to web resources is controlled according to the rule.
- **Rule schedule.** You can specify the rule schedule. The rule schedule determines the time span during which Kaspersky Endpoint Security monitors access to web resources covered by the rule.

After Kaspersky Endpoint Security is installed, the list of rules of the Web Control component is not blank. Two rules are preset:

- The Scenarios and Style Tables rule, which grants all users access at all times to web resources whose addresses contain the names of files with the css, js, or vbs extensions. For example: <http://www.example.com/style.css>, <http://www.example.com/style.css?mode=normal>.
- The "Default" rule, which grants all users access to any web resources at any time.

ACTIONS WITH WEB RESOURCE ACCESS RULES

You can take the following actions on web resource access rules:

- Add a new rule.
- Edit a rule.
- Assign priority to a rule.

The priority of a rule is defined by the position of the line which contains a brief description of this rule, in the settings window of the Web Control component, in the **Access rules sorted by priority** table. This means that a rule that is higher in the **Access rules sorted by priority** table has a higher priority than one that is located lower.

If the web resource that the user attempts to access matches the parameters of several rules, Kaspersky Endpoint Security performs an action according to the rule with the highest priority.

- Test a rule.

You can check the consistency of rules by using the Rules diagnostics service.

- Enable and disable a rule.

A web resource access rule can be enabled (operation status: *On*) or disabled (operation status: *Off*). By default, after a rule is created, it is enabled (operation status: *On*). You can disable the rule.

- Delete a rule.

IN THIS SECTION:

Adding and editing a web resource access rule	151
Assigning priorities to web resource access rules	152
Testing web resource access rules	153
Enabling and disabling a web resource access rule.....	154

ADDING AND EDITING A WEB RESOURCE ACCESS RULE

➤ *To add or edit a web resource access rule:*

1. Open the application settings window. (see the section "Application settings window" on page [48](#))
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the settings of the Web Control component are displayed.

3. Do one of the following:
 - To add a rule, click the **Add** button.
 - To edit a rule, select it in the **Access rules sorted by priority** table and click the **Edit** button.

The **Rule of access to web resources** window opens.

4. Specify or edit the settings of the rule. To do so:
 - a. In the **Name** field, enter or edit the name of the rule.
 - b. From the **Filter content** drop-down list, select the required option:
 - **Any content.**
 - **By content categories.**
 - **By types of data.**
 - **By content categories and types of data.**

If an option other than **Any content** is selected, a section for selecting content categories and / or data type categories opens. Select the check boxes next to the names of the required content categories and / or data type categories.

Selecting the check box next to the name of a content category and / or data type category means that Kaspersky Endpoint Security applies the rule to control access to web resources that belong to the selected content categories and / or data type categories.

- c. From the **Apply to addresses** drop-down list, select the required option:
 - **To all addresses.**

- **To individual addresses.**

If the **To individual addresses** option is selected, a section opens where you create a list of web resources. You can create and edit the list of web resources by using the **Add**, **Edit**, and **Delete** buttons.

- d. Select the **Specify users and / or groups** check box and click the **Select** button.

The standard **Select Users or Groups** window in Microsoft Windows opens.

- e. Specify or edit the list of users and / or groups of users for which access to web resources that are described by the rule is to be allowed or blocked.

- f. From the **Action** drop-down list, select the required option:

- **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 may be dangerous 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.

- g. In the **Rule schedule** drop-down list that opens, select the name of the necessary schedule or create a new schedule that is based on the selected rule schedule. To do so:

1. Opposite the **Rule schedule** drop-down list, click the **Settings** button.

The **Rule schedule** window opens.

2. To supplement the rule schedule with a time span during which the rule does not apply, in the table that shows the rule schedule, click the table cells that correspond to the time and day of the week that you want to select.

The color of the cells turns gray.

3. To substitute a time span during which the rule applies with a time span during which the rule does not apply, click the gray cells in the table which correspond to the time and day of the week that you want to select.

The color of the cells turns green.

4. If you are creating a rule schedule that is based on the schedule of the Always rule that is created by default, click **OK** or **Save as**. If you are creating a rule schedule based on the schedule of a rule that was not created by default, click **Save as**.

The **Rule schedule name** window opens.

5. Type a rule schedule name or leave the default name that is suggested.
6. Click **OK**.

5. In the **Rule of access to web resources** window, click **OK**.

6. To save changes, click the **Save** button.

ASSIGNING PRIORITIES TO WEB RESOURCE ACCESS RULES

You can assign priorities to each rule from the list of rules, by arranging the rules in a certain order.

➤ *To assign a priority to a web resource access rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.
In the right part of the window, the settings of the Web Control component are displayed.
3. In the right part of the window, select the rule for which you want to change the priority.
4. Use the **Move up** and **Move down** buttons to move the rule to the required rank in the list of rules.
5. Repeat steps 3–4 for the rules whose priority you want to change.
6. To save changes, click the **Save** button.

TESTING WEB RESOURCE ACCESS RULES

To check the consistency of Web Control rules, you can test them. To do this, the Web Control component includes a Rules diagnostics service.

➤ *To test the web resource access rules:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.
In the right part of the window, the settings of the Web Control component are displayed.
3. In the right part of the window, click the **Diagnostics** button.
The **Rules diagnostics** window opens.
4. Fill in the fields in the **Conditions** section:
 - a. If you want to test the rules that Kaspersky Endpoint Security uses to control access to a specific web resource, select the **Specify address** check box. Enter the address of the web resource in the field below.
 - b. If you want to test the rules that Kaspersky Endpoint Security uses to control access to web resources for specified users and / or groups of users, specify a list of users and / or groups of users.
 - c. If you want to test the rules that Kaspersky Endpoint Security uses to control access to web resources of specified content categories and / or data type categories, from the **Filter content** drop-down list, select the required option (**By content categories**, **By types of data**, or **By content categories and types of data**).
 - d. If you want to test the rules with account of the time and day of the week when an attempt is made to access the web resource(s) that are specified in the rule diagnostics conditions, select the **Include time of access attempt** check box. Then specify the day of the week and the time.
5. Click the **Test** button.

Test completion is followed by a message with information about the action that is taken by Kaspersky Endpoint Security, according to the first rule that is triggered on the attempt to access the specified web resource(s) (allow, block, or warn). The first rule to be triggered is the one with a rank on the list of Web Control rules which is higher than that of other rules meeting the diagnostics conditions. The message is displayed on the right of the **Test** button. The following table lists the remaining triggered rules, specifying the action taken by Kaspersky Endpoint Security. The rules are listed in the order of declining priority.

ENABLING AND DISABLING A WEB RESOURCE ACCESS RULE

➤ *To enable or disable a web resource access rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the settings of the Web Control component are displayed.
3. In the right part of the window, select the rule that you want to enable or disable.
4. In the **Status** column, do the following:
 - If you want to enable the use of the rule, select the *On* value.
 - If you want to disable the use of the rule, select the *Off* value.
5. To save changes, click the **Save** button.

EXPORTING AND IMPORTING THE LIST OF WEB RESOURCE ADDRESSES

If you have created a list of web resource addresses in a web resource access rule, you can export it to a .txt file. You can subsequently import the list from this file to avoid creating a new list of web resource addresses manually when configuring an access rule. The option of exporting and importing the list of web resource addresses may be useful if, for example, you create access rules with similar parameters.

➤ *To export a list of web resource addresses to a file:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the settings of the Web Control component are displayed.
3. Select the rule whose list of web resource addresses you want to export to a file.
4. Click the **Edit** button.

The **Rule of access to web resources** window opens.
5. If you do not want to export the entire list of web resource addresses, but rather just a part of it, select the required web resource addresses.

6. To the right of the field with the list of web resource addresses, click the  button.

The action confirmation window opens.

7. Do one of the following:
 - If you want to export only the selected items of the web resource address list, in the action confirmation window, click the **Yes** button.
 - If you want to export all items of the list of web resource addresses, in the action confirmation window, click the **No** button.

The standard **Save as** window of Microsoft Office opens.

- In the **Save as** Microsoft Windows window, select the file to which you want to export the list of web resource addresses. Click the **Save** button.

➔ *To import the list of web resource addresses from a file into a rule:*

- Open the application settings window (on page [48](#)).
- In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the settings of the Web Control component are displayed.

- Do one of the following:
 - If you want to create a new web resource access rule, click the **Add** button
 - Select the web resource access rule that you want to edit. Then click the **Edit** button.

The **Rule of access to web resources** window opens.

- Do one of the following:
 - If you are creating a new web resource access rule, select **To individual addresses** from the **Apply to addresses** drop-down list.
 - If you are editing a web resource access rule, go to step 5 of these instructions.

- To the right of the field with the list of web resource addresses, click the  button.

If you are creating a new rule, the standard Microsoft Windows **Open file** window opens.

If you are editing a rule, a window requesting your confirmation opens.

- Do one of the following:
 - If you are editing a new web resource access rule, go to step 7 of these instructions.
 - If you are editing a web resource access rule, do one of the following actions in the action confirmation window:
 - If you want to add imported items of the list of web resource addresses to the existing ones, click the **Yes** button.
 - If you want to delete the existing items of the list of web resource addresses and to add the imported ones, click the **No** button.

The **Open file** window in Microsoft Windows opens.

- In the **Open file** window in Microsoft Windows, select a file with a list of web resource addresses to import.
- Click the **Open** button.
- In the **Rule of access to web resources** window, click **OK**.

EDITING MASKS FOR WEB RESOURCE ADDRESSES

Using a *web resource address mask* (also referred to as "address mask") may be useful if you need to enter numerous similar web resource addresses when creating a web resource access rule. If crafted well, one address mask can replace a large number of web resource addresses.

When creating an address mask, keep in mind the following rules:

1. The * character replaces any sequence that contains zero or more characters.

For example, if you enter the *abc* address mask, the access rule is applied to all web resources that contain the sequence abc. Example: http://www.example.com/page_0-9abcdef.html.

The ? character is treated as a question mark. It is not regarded as any single character, according to the rules for creating address masks in the Web Anti-Virus component.

To include the * character in an address mask, enter two * characters, not the sequence *, as in the rules for creating address masks in the Web Anti-Virus component.

2. The `www.` character sequence at the start of the address mask is interpreted as a *. sequence.

Example: the address mask `www.example.com` is treated as `*.example.com`.

3. If an address mask does not start with the * character, the content of the address mask is equivalent to the same content with the *. prefix.

4. The character sequence *. at the start of the mask is interpreted as *. or an empty string.

Example: the address mask http://www.*.example.com covers the address <http://www2.example.com>.

5. If an address mask ends with a character other than / or *, the content of the address mask is equivalent to the same content with the /* postfix.

Example: the address mask <http://www.example.com> covers such addresses as <http://www.example.com/abc>, where a, b, and c are any characters.

6. If an address mask ends with the / character, the content of the address mask is equivalent to the same content with the /* postfix.

7. The character sequence /* at the end of an address mask is interpreted as /* or an empty string.

8. Web resource addresses are verified against an address mask, taking into account the protocol (http or https):

- If the address mask contains no network protocol, this address mask covers addresses with any network protocol.

Example: the address mask `example.com` covers the addresses <http://example.com> and <https://example.com>.

- If the address mask contains a network protocol, this address mask only covers addresses with the same network protocol as that of the address mask.

Example: the address mask http://*.example.com covers the address <http://www.example.com> but does not cover <https://www.example.com>.

9. An address mask that is in double quotes is treated without considering any additional replacements, except the * character if it has been initially included in the address mask. This means that such address masks are not covered by rules 5 and 7.

10. The user name and password, connection port, and character case are not taken into account during comparison with the address mask of a web resource.

Table 3. Examples of how to use rules for creating address masks

No.	ADDRESS MASK	ADDRESS OF WEB RESOURCE TO VERIFY	IS THE ADDRESS COVERED BY THE ADDRESS MASK	COMMENT
1	*.example.com	http://www.123example.com	No	See rule 1.
2	*.example.com	http://www.123.example.com	Yes	See rule 1.
3	*example.com	http://www.123example.com	Yes	See rule 1.
4	*example.com	http://www.123.example.com	Yes	See rule 1.
5	http://www.*.example.com	http://www.123example.com	No	See rule 1.
6	www.example.com	http://www.example.com	Yes	See rules 2, 1.
7	www.example.com	https://www.example.com	Yes	See rules 2, 1.
8	http://www.*.example.com	http://123.example.com	Yes	See rules 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Yes	See rules 2, 5, 1.
10	example.com	http://www.example.com	Yes	See rules 3, 1.
11	http://example.com/	http://example.com/abc	Yes	See rule 6.
12	http://example.com/*	http://example.com	Yes	See rule 7.
13	http://example.com	https://example.com	No	See rule 8.
14	"example.com"	http://www.example.com	No	See rule 9.
15	"http://www.example.com"	http://www.example.com/abc	No	See rule 9.
16	"*.example.com"	http://www.example.com	Yes	See rules 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Yes	See rules 1, 9.
18	"www.example.com"	http://www.example.com ; https://www.example.com	Yes	See rules 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	No	An address mask contains more information than the address of a web resource.

EDITING TEMPLATES OF WEB CONTROL MESSAGES

Depending on the type of action that is specified in the properties of Web Control rules, Kaspersky Endpoint Security displays a message of one of the following types when users attempt to access Internet resources (the application substitutes an HTML page with a message for the HTTP server response):

- **Warning message.** Such a message warns the user that a web resource may be dangerous and / or out of compliance with corporate policy. Kaspersky Endpoint Security displays a warning message if the **Warn** option is selected from the **Action** drop-down list in the properties of the rule that describes this web resource.

If you think that the warning is mistaken, you may click the link from the warning message to open a pre-generated complaint message and send it to the LAN administrator.

- **Message informing of blocking of a web resource.** Kaspersky Endpoint Security displays a message that informs that a web resource is blocked, if the **Block** option is selected from the **Action** drop-down list in the properties of the rule that describes this web resource.

If you think that the web resource is blocked by mistake, you may click the link from the message that informs of the blocking of the web resource to open a pre-generated complaint message and send it to the LAN administrator.

Special templates are provided for a warning message, a message informing that a web resource is blocked, and a complaint message to send to the LAN administrator. You can modify their content.

➤ *To change the template for Web Control messages:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the settings of the Web Control component are displayed.
3. In the right part of the window, click the **Templates** button.

The **Templates** window opens.
4. Do one of the following:
 - If you want to edit the template of the message that warns the user that a web resource is a possible threat, select the **Warning** tab.
 - If you want to edit the template of the message that informs the user that access to a web resource is blocked, select the **Blockage** tab.
 - If you want to edit the template of the complaint message, select the **Complaint** tab.
5. Edit the message template. To do this, use the **By default** and **Variables** buttons.
6. Click **OK**.
7. To save changes, click the **Save** button.

UPDATING DATABASES AND APPLICATION SOFTWARE MODULES

This section contains information about database and application module updates (also called "updates"), and instructions on how to configure update settings.

IN THIS SECTION:

About database and application module updates.....	159
About update sources	160
Update settings configuration.....	160
Starting and stopping an update task.....	165
Rolling back the last update	166
Configuring proxy server settings.....	166
Enabling and disabling scanning of files in Quarantine after an update	167

ABOUT DATABASE AND APPLICATION MODULE UPDATES

Updating the databases and application modules of Kaspersky Endpoint Security ensures up-to-date protection on your computer. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Endpoint Security databases contain information about threats and ways of neutralizing them. To detect new threats quickly, you are urged to regularly update the databases and application modules.

Regular updating requires an active license for application use. If no license is active, you will be able to perform an update only once.

The main update source for Kaspersky Endpoint Security is Kaspersky Lab update servers.

Your computer must be connected to the Internet to successfully download the update package from Kaspersky Lab update servers. By default, the Internet connection settings are determined automatically. If you use a proxy server, you need to adjust the connection settings.

While performing an update, the following objects are downloaded and installed on your computer:

- **Kaspersky Endpoint Security databases.** Computer protection is provided, thanks to databases that contain threat signatures and information about how to neutralize threats. Protection components use this information when searching for and neutralizing infected files on your computer. The databases are constantly supplemented with records of new threats. Therefore we recommend that you update the databases regularly.

In addition to the Kaspersky Endpoint Security databases, the network drivers that enable the application's components to intercept network traffic are updated.

- **Application modules.** In addition to the databases of Kaspersky Endpoint Security, you can also update the application modules. Updating the application modules fixes vulnerabilities in Kaspersky Endpoint Security, adds new functions, or enhances existing functions.

While updating, the application modules and databases on your computer are compared against the up-to-date version at the update source. If your current databases and application modules differ from their respective up-to-date versions, the missing portion of the updates is installed on your computer.

If the databases are obsolete, the update package may be large, which may cause additional Internet traffic (up to several dozen MB).

Information on the current status of Kaspersky Endpoint Security databases is shown in **Update**, in the **Tasks** section on the **Protection and Control** tab of the main application window.

Information on the update results and events that occur during the execution of the update task is logged in a Kaspersky Endpoint Security report (see the section "Managing reports" on page [193](#)).

ABOUT UPDATE SOURCES

An *update source* is a resource that contains updates for databases and application modules of Kaspersky Endpoint Security.

Update sources include FTP or HTTP servers (such as Kaspersky Security Center and Kaspersky Lab update servers) and network or local folders.

If you do not have access to Kaspersky Lab update servers (for example, Internet access is limited), you can contact Kaspersky Lab headquarters (<http://www.kaspersky.com/contacts>) to request contact information for Kaspersky Lab partners. Kaspersky Lab partners will provide you with updates on a removable disk.

When ordering updates on a removable disk, please specify whether you also need application module updates.

SEE ALSO:

Adding an update source	161
Selecting the update server region.....	162
Configuring updates from a shared folder	162

UPDATE SETTINGS CONFIGURATION

You can perform the following actions to configure the update settings:

- Add new update sources.

The default list of update sources includes Kaspersky Security Center and Kaspersky Lab update servers. You can add other update sources to the list. You can specify HTTP/FTP servers and shared folders as update sources.

If several resources are selected as update sources, Kaspersky Endpoint Security tries to connect to them one after another, starting from the top of the list, and performs the update task by retrieving the update package from the first available source.

If you select a resource outside the LAN as the update source, you must have an Internet connection to perform an update.

- Select the region of the Kaspersky Lab update server.

If you use Kaspersky Lab update servers as an update source, you can select the location of the Kaspersky Lab update server that is used to download the update package. Kaspersky Lab update servers are located in several countries. Using the nearest Kaspersky Lab update servers helps to reduce the time that is spent on retrieving an update package.

By default, the application uses information about the current region from the operating system's registry.

- Configure updating of Kaspersky Endpoint Security from a shared 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 this end, one of the computers on your LAN receives an up-to-date update package from the Kaspersky Security Center server or 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.

- Select the update task run mode.

If it is not possible to run the update task for any reason (for example, the computer is not on at that time), you can configure the skipped task to be start automatically as soon as this becomes possible.

You can postpone running the update task after the application starts if you have selected the **By schedule** update task run mode, and if the start time of Kaspersky Endpoint Security matches the update task start schedule. The update task can only be run after the specified time interval elapses after the startup of Kaspersky Endpoint Security.

- Configure the update task to run under the rights of a different user account.

IN THIS SECTION:

Adding an update source	161
Selecting the update server region.....	162
Configuring updates from a shared folder	162
Selecting the update task run mode	164
Starting an update task under the rights of a different user account	165

ADDING AN UPDATE SOURCE

➔ *To add an update source:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.
In the right part of the window, the Application Update Settings are displayed.
3. In the **Run mode and update source** section, click the **Update source** button.
The **Source** tab of the **Update** window opens.
4. On the **Source** tab, click the **Add** button.
The **Select update source** window opens.
5. In the **Select update source** window, select a folder with the update package or enter the full path to the folder in the **Source** field.

6. Click **OK**.
7. In the **Update** window, click **OK**.
8. To save changes, click the **Save** button.

SEE ALSO:

About update sources	160
Selecting the update server region.....	162
Configuring updates from a shared folder	162

SELECTING THE UPDATE SERVER REGION

➤ *To select the update server region:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.
In the right part of the window, the Application Update Settings are displayed.
3. In the **Run mode and update source** section, click the **Update source** button.
The **Source** tab of the **Update** window opens.
4. On the **Source** tab, in the **Regional settings** section, select **Select from the list**.
5. In the drop-down list, select the country that is nearest to your current location.
6. Click **OK**.
7. To save changes, click the **Save** button.

SEE ALSO:

About update sources	160
Adding an update source	161
Configuring updates from a shared folder	162

CONFIGURING UPDATES FROM A SHARED FOLDER

Configuring the updates of Kaspersky Endpoint Security from a shared folder consists of the following steps:

1. Enabling the copying of an update package to a shared folder on one of the computers on the local area network.
2. Configuring updates of Kaspersky Endpoint Security from the specified shared folder to the remaining computers on the local area network.

➤ *To enable copying of the update package to the shared folder:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.
In the right part of the window, the Application Update Settings are displayed.
3. In the **Additional** section, select the **Copy updates to folder** check box.
4. Specify the path to the shared folder where the update package is to be placed. You can do this in one of the following ways:
 - Enter the path to the shared folder in the field under the **Copy updates to folder** check box.
 - Click the **Browse** button. Then, in the **Select folder** window that opens, select the necessary folder and click **OK**.
5. To save changes, click the **Save** button.

➤ *To configure updating of Kaspersky Endpoint Security from a shared folder:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.
In the right part of the window, the Application Update Settings are displayed.
3. In the **Run mode and update source** section, click the **Update source** button.
The **Source** tab of the **Update** window opens.
4. On the **Source** tab, click the **Add** button.
The **Select update source** window opens.
5. In the **Select update source** window, select the shared folder that contains the update package or enter the full path to the shared folder in the **Source** field.
6. Click **OK**.
7. On the **Source** tab, clear the check boxes next to the names of the update sources that you have not specified as the shared folder.
8. Click **OK**.
9. To save changes, click the **Save** button.

SEE ALSO:

About update sources	160
Adding an update source	161
Selecting the update server region.....	162

SELECTING THE UPDATE TASK RUN MODE

➤ To select the update task run mode:

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.
In the right part of the window, the Application Update Settings are displayed.
3. Click the **Run mode** button.
The **Run mode** tab opens in the **Update** window.
4. In the **Run mode** section, select one of the following options for starting an update task:
 - If you want Kaspersky Endpoint Security to run the update task depending on whether or not an update package is available from the update source, select **Automatically**. The frequency of checks by Kaspersky Endpoint Security for update packages increases during virus outbreaks and is less at other times.
 - If you want to start an update task manually, select **Manually**.
 - If you want to configure a startup schedule for the update task, select **By schedule**.
5. Do one of the following:
 - If you have selected the **Automatically** or **Manually** option, go to step 6 in the instructions.
 - If you have selected the **By schedule** option, specify the settings of the update task run schedule. To do so:
 - a. In the **Frequency** drop-down list, specify when to start the update task. Select one of the following options: **Minutes**, **Hours**, **Days**, **Every week**, **At a specified time**, **Every month**, or **After application startup**.
 - b. Depending on the item that is selected from the **Frequency** drop-down list, specify values for the settings that define the startup time of the update task.
 - c. In the **Postpone run after application startup for** field, specify the time interval by which the start of the update task is postponed after the startup of Kaspersky Endpoint Security.

If the **After application startup** item is selected from the **Frequency** drop-down list, the **Postpone run after application startup for** field is not available.
 - d. If you want Kaspersky Endpoint Security to run skipped update tasks as soon as possible, select the **Run skipped tasks** check box.

If **Hours**, **Minutes** or **After application startup** is selected from the **Frequency** drop-down list, the **Run skipped tasks** check box is unavailable.
6. Click **OK**.
7. To save changes, click the **Save** button.

SEE ALSO:

Starting and stopping an update task [165](#)

STARTING AN UPDATE TASK UNDER THE RIGHTS OF A DIFFERENT USER ACCOUNT

By default, the Kaspersky Endpoint Security update task is started on behalf of the user whose account you have used to log in to the operating system. However, Kaspersky Endpoint Security can be updated from an update source that you cannot access due to a lack of the required rights (for example, from a shared folder that contains an update package) or not having the rights of an authorized proxy server user. In the Kaspersky Endpoint Security settings, you can specify a user that has such rights and start the Kaspersky Endpoint Security update task under that user account.

➤ *To start an update task under a different user account:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.
In the right part of the window, the Application Update Settings are displayed.
3. In the **Run mode and update source** section, click the **Run mode** button.
The **Run mode** tab opens in the **Update** window.
4. On the **Run mode** tab, in the **User account** section, select the **Start task as** check box.
5. In the **Name** field, enter the account of the user whose rights are necessary for accessing the update source.
6. In the **Password** field, enter the password of the user whose rights are necessary for accessing the update source.
7. Click **OK**.
8. To save changes, click the **Save** button.

STARTING AND STOPPING AN UPDATE TASK

Regardless of the selected update task run mode, you can start or stop a Kaspersky Endpoint Security update task at any time.

To download an update package from Kaspersky Lab servers, an Internet connection is required.

➤ *To start or stop an update task:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Tasks** section.
The **Tasks** section opens.
4. Right-click to bring up the context menu of the line with the update task name.
Clicking this line opens a menu of actions to take on the update task.
5. Do one of the following:
 - If you want to start the update task, select **Start update** from the menu.

The progress status of the update task, which is displayed on the right of the **Update** button, changes to *Running*.

- If you want to stop the update task, select **Stop update** from the menu.

The progress status of the update task, which is displayed on the right of the **Update** button, changes to *stopped*.

ROLLING BACK THE LAST UPDATE

After the databases and application modules are updated for the first time, the function of rolling back the databases and application modules to their previous versions becomes available.

Each time that a user starts the update process, Kaspersky Endpoint Security creates a backup copy of the current databases and application modules. This lets you roll back the databases and application modules to their previous versions when necessary. Rolling back the last update is useful, for example, when the new database version contains an invalid signature that causes Kaspersky Endpoint Security to block a safe application.

➔ *To roll back the last update:*

1. Open the main application window.
2. Select the **Protection and Control** tab.
3. Click the **Tasks** section.

The **Tasks** section opens.

4. Right-click to bring up the context menu of the **Update** task.
5. Select **Roll back update**.

CONFIGURING PROXY SERVER SETTINGS

➔ *To configure proxy server settings:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.

In the right part of the window, the Application Update Settings are displayed.

3. In the **Proxy server** section, click the **Settings** button.

The **Proxy server** tab opens in the **Update** window.

4. On the **Proxy server** tab, select the **Use proxy server** check box.
5. Specify proxy server settings.
6. Click **OK**.
7. To save changes, click the **Save** button.

You can also configure the proxy server settings in the main application window, on the **Settings** tab, in the **Advanced settings** section.

ENABLING AND DISABLING SCANNING OF FILES IN QUARANTINE AFTER AN UPDATE

If Kaspersky Endpoint Security detects signs of infection when scanning a file but is unable to determine which specific malicious programs have infected it, Kaspersky Endpoint Security moves this file to Quarantine. Kaspersky Endpoint Security may later identify the threat and neutralize it after the databases and application modules are updated. You can enable the automatic scanning of files in Quarantine after each update of the databases and application modules.

We recommend that you regularly scan files in Quarantine. Scanning may change the status of files. Some files can then be disinfected and restored to their original locations so that you can continue using them.

➤ *To enable scanning of quarantined files after updates:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Reports and Storages**.

In the right part of the window, the management settings for reports and storages are displayed.
3. In the **Local quarantine and backup** section, do one of the following:
 - To enable the scanning of quarantined files after each update of Kaspersky Endpoint Security, select the **Rescan Quarantine after update** check box.
 - To disable the scanning of quarantined files after each update of Kaspersky Endpoint Security, clear the **Rescan Quarantine after update** check box.
4. To save changes, click the **Save** button.

SCANNING THE COMPUTER

Scanning your computer for viruses and other types of malware is essential to computer security. You are urged to regularly scan your computer for viruses and other malware to rule out the spread of malicious programs that have not been detected by protection components, for example, due to a low security level setting or for other reasons.

This section describes the specifics and settings of scan tasks, security levels, scan methods and technologies, and instructions on handling files which Kaspersky Endpoint Security has not processed when scanning the computer for viruses and other malware.

IN THIS SECTION:

About scan tasks.....	168
Starting or stopping a scan task.....	169
Configuring scan task settings.....	169
Handling unprocessed files.....	178

ABOUT SCAN TASKS

To find viruses and other types of malware, Kaspersky Endpoint Security includes the following tasks:

- **Full Scan.** A thorough scan of the entire computer. By default, Kaspersky Endpoint Security scans the following objects:
 - System memory
 - Objects that are loaded at startup of the operating system
 - Operating system backup
 - All hard and removable drives
- **Critical Areas Scan.** By default, Kaspersky Endpoint Security scans objects that are loaded at startup of the operating system.
- **Custom Scan.** Kaspersky Endpoint Security scans the objects that are selected by the user. You can scan any object from the following list:
 - System memory
 - Objects that are loaded at startup of the operating system
 - Operating system backup
 - Mail databases
 - All hard, removable, and network drives
 - Any selected file

The Full Scan and Critical Areas Scan tasks are somewhat different than the others. For these tasks, it is not recommended to edit the lists of objects to scan.

After scan tasks start, their completion progress is displayed in the field next to the name of the running scan task, in the **Tasks** section on the **Protection and Control** tab of the main window of Kaspersky Endpoint Security.

Information on the scan results and events that have occurred during the performance of scan tasks is logged in a Kaspersky Endpoint Security report.

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 (on page [46](#)).
2. Select the **Protection and Control** tab.
3. Click the **Tasks** section.

The **Tasks** section opens.

4. Right-click to bring up the context menu of the line with the scan task name.

A menu with scan task actions opens.

5. Do one of the following:

- If you want to start the scan task, select **Start scanning** from the menu.

The task progress status that is displayed on the right of the button with the name of this scan task changes to *Running*.

- If you want to stop the scan task, select **Stop scanning** from the menu.

The task progress status that is displayed on the right of the button with the name of this scan task changes to *Stopped*.

CONFIGURING SCAN TASK SETTINGS

To configure scan task settings, you can perform the following:

- Change the file security level.

You can select one of the preset file security levels or configure security level settings on your own. If you have changed the file security level settings, you can always revert to the recommended file security level settings.

- Change the action that Kaspersky Endpoint Security performs if it detects an infected file.
- Edit the scan scope.

You can expand or restrict the scan scope by adding or removing scan objects, or by changing the type of files to be scanned.

- Optimize scanning.

You can optimize file scanning: reduce scanning time and increase the operating speed of Kaspersky Endpoint Security. This can be achieved by scanning only new files and those files that have been modified since the previous scan. This mode applies both to simple and to compound files. You can also set a limit for scanning a single file. When the specified time interval expires, Kaspersky Endpoint Security excludes the file from the current scan (except archives and objects that include several files).

- Configure scanning of compound files.
- Configure the use of scan methods.

When active, Kaspersky Endpoint Security uses signature analysis. During signature analysis, Kaspersky Endpoint Security matches the detected object with records in its database. Following the recommendations of Kaspersky Lab's experts, signature analysis is always enabled.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky Endpoint Security analyzes the activity of objects in the operating system. Heuristic analysis can detect new malicious objects for which there are currently no records in the Kaspersky Endpoint Security database.

- Configure the use of scan technologies.

You can enable the use of the iChecker and iSwift technologies. These technologies optimize the speed of scanning files, by excluding files that have not been modified since the most recent scan.

- Select the scan task run mode.

If it is impossible to run the scan task for any reason (for example, the computer is off at that time), you can configure the skipped task to be run automatically as soon as this becomes possible.

You can postpone the scan task start after application startup if you have selected the **By schedule** update task run mode and the Kaspersky Endpoint Security startup time matches the scan task run schedule. The scan task can only be run after the specified time interval elapses after the startup of Kaspersky Endpoint Security.

- Configure the scan task to run under a different user account.
- Specify the settings for scanning removable drives when they are connected.

IN THIS SECTION:

Changing the file security level.....	171
Changing the action to take on infected files.....	171
Editing the scan scope	172
Optimizing file scanning	173
Scanning compound files	174
Selecting the scan method	175
Using scan technologies	175
Selecting the scan task run mode	175
Starting a scan task under the account of a different user	176
Scanning removable drives when they are connected to the computer	177

CHANGING THE FILE SECURITY LEVEL

To perform scan tasks, Kaspersky Endpoint Security uses various combinations of settings. These groups of settings are called *file security levels*. There are three pre-installed file security levels: **High**, **Recommended**, and **Low**. The **Recommended** file security level is considered the optimal group of settings, and is recommended by Kaspersky Lab.

➤ *To change the file security level:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed file security levels (**High**, **Recommended**, or **Low**), use the slider to select one.
 - If you want to configure a custom file security level, click the **Settings** button and, in the window that opens, specify the settings with the name of a scan task.

After you configure a custom file security level, the name of the file security level in the **Security level** section changes to **Custom**.
 - If you want to change the file security level to **Recommended**, click the **Default** button.
4. To save changes, click the **Save** button.

CHANGING THE ACTION TO TAKE ON INFECTED FILES

➤ *To change the action to take on infected files:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

3. In the **Action on threat detection** section, select the required option:
 - **Select action automatically.**
 - **Perform action: Disinfect. Delete if disinfection fails.**
 - **Perform action: Disinfect.**
 - **Perform action: Delete.**
 - **Perform action: Inform.**
4. To save changes, click the **Save** button.

EDITING THE SCAN SCOPE

The scan scope refers to the location and type of files (for example, all hard drives, startup objects, and email databases) that Kaspersky Endpoint Security scans when performing a scan task.

To create the scan scope:

- Edit the list of objects to be scanned.
- Select a type of files to be scanned.

➔ *To edit the list of objects to scan:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

3. Click the **Scan objects** button.

The **Scan scope** window opens.

4. In the **Objects to scan** list, do one of the following actions:

- If you want to add a new object to the list of objects for scanning, click the **Add** button.
- If you want to change the location of an object, select one from the list of objects to be scanned and click the **Edit** button.

The **Select object to scan** window opens.

- If you want to delete an object from the list of objects to be scanned, select one from the list of objects to be scanned and click the **Delete** button.

A window for confirming deletion opens.

You cannot remove or edit objects that are included in the list of objects to be scanned by default.

5. Do one of the following:

- If you want to add a new object or change the location of an object from the list of objects to be scanned, select one in the **Select object to scan** window and click the **Add** button.

All objects that are selected in the **Select object to scan** window are displayed in the **File Anti-Virus** window, in the **Protection scope** list.

Then click **OK**.

- If you want to remove an object, click the **Yes** button in the window for confirming removal.

6. If necessary, repeat steps 4–5 for adding, moving, or removing objects from the list of objects to be scanned.
7. To exclude an object from the list of objects to be scanned, clear the check box next to the object on the **Protection scope** list. The object remains on the list of objects to be scanned, but it is not scanned when the scan task runs.
8. Click **OK**.

9. To save changes, click the **Save** button.

➤ *To select the type of scanned objects:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

3. In the **Security level** section, click the **Settings** button.

A window with the name of the selected scan task opens.

4. In the window with the name of the selected scan task, select the **Scope** tab.
5. In the **File types** section, specify the type of files that you want to scan when the selected scan task runs:

- If you want to scan all files, select **All files**.
- If you want to scan files of formats which are the most vulnerable to infection, select **Files scanned by format**.
- If you want to scan files with extensions that are the most vulnerable to infection, select **Files scanned by extension**.

When selecting the type of files to scan, remember the following information:

- There are some file formats (such as .txt) for which the probability of intrusion of malicious code and its subsequent activation is quite low. At the same time, there are file formats that contain or may contain executable code (such as .exe, .dll, and .doc). The risk of intrusion and activation of malicious code in such files is quite high.
- An intruder may send a virus or another malicious program to your computer in an executable file that has been renamed with the .txt extension. If you select scanning of files by extension, such a file is skipped by the scan. If scanning of files by format is selected, then regardless of the extension, File Anti-Virus analyzes the file header. This analysis may reveal that the file is in .exe format. Such a file is thoroughly scanned for viruses and other malware.

6. In the window with the name of a task, click the **OK** button.
7. To save changes, click the **Save** button.

OPTIMIZING FILE SCANNING

➤ *To optimize file scanning:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

3. In the **Security level** section, click the **Settings** button.

A window with the name of the selected scan task opens.

4. In the window that opens, select the **Scope** tab.

5. In the **Scan optimization** section, perform the following actions:
 - Select the **Scan only new and changed files** check box.
 - Select the **Skip objects scanned longer than** check box and specify the scan length for a single file (in seconds).
6. Click **OK**.
7. To save changes, click the **Save** button.

SCANNING COMPOUND FILES

A common technique of concealing viruses and other malware is to implant them in compound files, such as archives or databases. To detect viruses and other malware that are hidden in this way, the compound file must be unpacked, which may slow down scanning. You can limit the set of compound files to be scanned, thus speeding up scanning.

➤ *To configure scanning of compound files:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

3. In the **Security level** section, click the **Settings** button.

A window with the name of the selected scan task opens.

4. In the window that opens, select the **Scope** tab.
5. In the **Scan of compound files** section, specify which compound files you want to scan: archives, installer packages or embedded OLE objects, mail format files, or password-protected archives.
6. If the **Scan only new and changed files** check box is cleared in the **Scan optimization** section, you can specify for each type of compound file whether to scan all files of this type or new ones only. To make your choice, click the [all / new](#) link next to the name of a type of compound file. This link changes its value when you click it.

If the **Scan only new and changed files** check box is selected, only new files are scanned.

7. Click the **Additional** button.

The **Compound files** window opens.

8. In the **Size limit** section, do one of the following:
 - If you do not want to unpack large compound files, select the **Do not unpack large compound files** check box and specify the required value in the **Maximum file size** field.
 - If you want to unpack large compound files, clear the **Do not unpack large compound files** check box.

A file is considered large if its size exceeds the value in the **Maximum file size** field.

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.

9. Click **OK**.

10. In the window with the name of a scan task, click the **OK** button.
11. To save changes, click the **Save** button.

SELECTING THE SCAN METHOD

➤ *To use scan methods:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.
3. In the **Security level** section, click the **Settings** button.

A window with the name of the selected scan task opens.
4. In the window that opens, select the **Additional** tab.
5. If you want the application to use heuristic analysis when running the scan task, in the **Scan methods** section, select the **Heuristic analysis** check box. Then use the slider to set the level of detail of Heuristic Analysis: **light scan**, **medium scan**, or **deep scan**.
6. Click **OK**.
7. To save changes, click the **Save** button.

USING SCAN TECHNOLOGIES

➤ *To use scan technologies:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.
3. In the **Security level** section, click the **Settings** button.

A window with the name of the selected scan task opens.
4. In the window that opens, select the **Additional** tab.
5. In the **Scan technologies** section, select the check boxes next to the names of technologies that you want to use during the scan.
6. Click **OK**.
7. To save changes, click the **Save** button.

SELECTING THE SCAN TASK RUN MODE

➤ *To select the scan task run mode:*

1. Open the application settings window (on page [48](#)).

- In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required scan task (**Full Scan**, **Critical Areas Scan** or **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

- Click the **Run mode** button.

The **Run mode** tab opens in the window with the name of the selected task.

- In the **Run mode** section, select one of the following options for starting the scan task:

- If you want to start the scan task manually, select **Manually**.
- If you want to configure the startup schedule for the scan task, select **By schedule**.

- Do one of the following:

- If you have selected the **Manually** option, go to step 6 of these instructions.
- If you have selected the **By schedule** option, specify the settings of the scan task run schedule. To do so:
 - In the **Frequency** drop-down list, specify when the scan task is to be started. Select one of the following options: **Days**, **Every week**, **At a specified time**, **Every month**, **After application startup**, or **After every update**.
 - Depending on the item that is selected in the **Frequency** drop-down list, specify values for the settings that define the start time of the scan task.
 - If you want Kaspersky Endpoint Security to start skipped scan tasks as soon as possible, select the **Run skipped tasks** check box.

If **After application startup** or **After every update** is selected from the **Frequency** drop-down list, the **Run skipped tasks** check box is unavailable.

- If you want Kaspersky Endpoint Security to suspend scan tasks when computing resources are limited, select the **Suspend scanning when the screensaver is off and the computer is unlocked** check box. This run schedule option for the scan task helps to conserve computing resources.
- Click **OK**.
 - To save changes, click the **Save** button.

STARTING A SCAN TASK UNDER THE ACCOUNT OF A DIFFERENT USER

By default, a scan task is run under the account with which the user is logged in to the operating system. However, you may need to run a scan task under a different user account. You can specify a user who has the appropriate rights in the settings of the scan task and run the scan task under this user's account.

◆ *To configure the start of a scan task under a different user account:*

- Open the application settings window (on page [48](#)).
- In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the relevant scan task (**Full Scan**, **Critical Areas Scan**, **Custom Scan**).

In the right part of the window, the settings of the selected scan task are displayed.

- Click the **Run mode** button.

The **Run mode** tab opens in the window with the name of the selected scan task.

4. On the **Run mode** tab, in the **User account** section, select the **Start task as** check box.
5. In the **Name** field, enter the account of the user whose rights are necessary for starting the scan task.
6. In the **Password** field, enter the password of the user whose rights are necessary for starting the scan task.
7. Click **OK**.
8. To save changes, click the **Save** button.

SCANNING REMOVABLE DRIVES WHEN THEY ARE CONNECTED TO THE COMPUTER

Malicious programs that use operating system vulnerabilities to replicate via networks and removable media have become increasingly widespread in recent times. Kaspersky Endpoint Security allows you to scan removable drives that are connected to your computer for viruses and other malware.

➡ *To configure scanning of removable drives when they are connected:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Scheduled tasks** section.

In the right part of the window, the general settings of scheduled tasks are displayed.
3. In the **Scan removable drives on connection** section, in the **Actions on drive connection** dropdown list, select the required action:
 - **Do not scan.**
 - **Full Scan.**
 - **Quick Scan**
4. If you want Kaspersky Endpoint Security to scan removable drives of a size less or equal to a specified value, select the **Maximum drive size** check box and specify a value in megabytes in the field next to it.
5. To save changes, click the **Save** button.

HANDLING UNPROCESSED FILES

This section contains instructions on handling infected files which Kaspersky Endpoint Security has not processed while scanning the computer for viruses and other threats.

IN THIS SECTION:

About unprocessed files	178
Managing the list of unprocessed files	178

ABOUT UNPROCESSED FILES

Kaspersky Endpoint Security logs information about unprocessed files in which it detects an active threat. This information is recorded in the form of events in the list of unprocessed files.

An infected file is considered *processed* if Kaspersky Endpoint Security performs one of the following actions on the infected file according to the specified application settings while scanning the computer for viruses and other threats:

- Disinfect.
- Delete.
- Delete if disinfection fails.

An infected file is considered *unprocessed* if Kaspersky Endpoint Security for any reason fails to perform an action on the infected file according to the specified application settings while scanning the computer for viruses and other threats.

This situation is possible in the following cases:

- The scanned file is unavailable (for example, it is located on a network drive or on a removable drive without write privileges).
- The action that is selected in the **Action on threat detection** section for scan tasks is **Inform**, and the user selects the **Skip** action when a notification about the infected file is displayed.

You can manually start a Custom Scan task for files in the list of unprocessed files after updating databases and application modules. File status may change after the scan. You may perform the necessary actions on the files, depending on their status.

For example, you can perform the following actions:

- Delete files with *Infected* status (see the section "*Deleting files from the list of unprocessed files*" on page [181](#)).
- Restore infected files that contain important information and restore files that are marked as *Disinfected* or *Not infected* (see the section "*Restoring files from the list of unprocessed files*" on page [180](#)).
- Move files with *Potentially infected* status to Quarantine (see the section "*Moving a file to Quarantine*" on page [205](#)).

MANAGING THE LIST OF UNPROCESSED FILES

The list of unprocessed files appears in the form of a table. Each table row contains an event that involves an unprocessed file (also called an "unprocessed file event") and includes the type of threat that was detected in the file.

You can perform the following file operations while managing the list of unprocessed files:

- View the list of unprocessed files.
- Scan unprocessed files by using the current version of Kaspersky Endpoint Security databases and modules.
- Restore files from the list of unprocessed files to their original folders or to a different folder of your choice (when the original folder cannot be written to).
- Delete files from the list of unprocessed files.
- Open the folder where the unprocessed file was originally located.

You can also perform the following actions while managing data in the table:

- Filter unprocessed file events by column value or custom filter conditions.
- Use the unprocessed file event search function.
- Sort unprocessed file events.
- Change the order and set of columns that are displayed in the list of unprocessed files.
- Group unprocessed file events.

You can copy selected unprocessed file events to the clipboard, if necessary.

IN THIS SECTION:

Starting a Custom Scan task for unprocessed files	179
Restoring files from the list of unprocessed files	180
Deleting files from the list of unprocessed files	181

STARTING A CUSTOM SCAN TASK FOR UNPROCESSED FILES

You can start a Custom Scan task for unprocessed files manually, for example, after a scan is interrupted for any reason or if you want Kaspersky Endpoint Security to scan files after a database and application module update.

◆ *To start a Custom Scan of unprocessed files:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Unprocessed objects** tab.
4. In the table on the **Unprocessed objects** tab, select one or more file events that you want to scan. To select multiple events, highlight them while holding down the **CTRL** key.

5. Start the Custom Scan task in one of the following ways:
 - Click the **Rescan** button.
 - Right-click to display the context menu. Select **Rescan**.

When the scan is completed, a notification with the number of scanned files and the number of detected threats appears.

RESTORING FILES FROM THE LIST OF UNPROCESSED FILES

You can restore files from the list of unprocessed files, if necessary.

Kaspersky Lab specialists recommend that you restore files from the list of unprocessed files only if the files have received *Not infected* status.

➡ *To restore files from the list of unprocessed files:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Unprocessed objects** tab.
4. To restore all files:
 - a. Right-click anywhere in the table on the **Unprocessed objects** tab to display the context menu.
 - b. Select **Restore all**.

Kaspersky Endpoint Security moves all files from the list of unprocessed files to their original folders as long as the folders can be written to.

- c. If the original folder of a restored file cannot be written to, the standard **Save as** window of Microsoft Windows opens. This window lets you select the destination folder for the file.
5. To restore one or more files:
 - a. In the table on the **Unprocessed objects** tab, select one or more unprocessed file events that you want to restore from the list of unprocessed files. To select multiple unprocessed file events, select them while holding down the **CTRL** key.
 - b. Restore files in one of the following ways:
 - Click the **Restore** button.
 - Right-click to display the context menu. Select **Restore**.

Kaspersky Endpoint Security moves the selected files to their original folders as long as the folders can be written to.

- c. If the original folder of a restored file cannot be written to, the standard **Save as** window of Microsoft Windows opens. This window lets you select the destination folder for the file.

DELETING FILES FROM THE LIST OF UNPROCESSED FILES

You can delete an infected file from the list of unprocessed files. Before deleting the file, Kaspersky Endpoint Security creates a backup copy of the file and saves it in Backup in case you later need to restore the file (see the section "Restoring files from the list of unprocessed files" on page [180](#)).

➔ *To delete files from the list of unprocessed files:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Unprocessed objects** tab.
4. In the table on the **Unprocessed objects** tab, select one or more file events that you want to delete. To select multiple events, select them while holding down the **CTRL** key.
5. Delete files in one of the following ways:
 - Click the **Delete** button.
 - Right-click to display the context menu. Select **Delete**.

Kaspersky Endpoint Security creates a backup copy of each file and saves the copy in Backup (see the section "About Quarantine and Backup" on page [202](#)). Kaspersky Endpoint Security then deletes the selected files from the list of unprocessed files.

VULNERABILITY SCAN

This section contains information about Vulnerability Monitor, the specifics and settings of the Vulnerability Scan task, and instructions on managing the list of vulnerabilities that are detected by Kaspersky Endpoint Security while running the Vulnerability Scan task.

IN THIS SECTION:

About Vulnerability Monitor	182
Enabling and disabling Vulnerability Monitor	182
Viewing information about vulnerabilities of running applications.....	183
About the Vulnerability Scan task.....	184
Starting or stopping the Vulnerability Scan task.....	184
Creating the vulnerability scan scope.....	185
Selecting the Vulnerability Scan task run mode	185
Configuring the launch of the Vulnerability Scan task under a different user account.....	186
Handling detected vulnerabilities.....	188

ABOUT VULNERABILITY MONITOR

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 that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

The Vulnerability Monitor component runs a real-time vulnerability scan of applications that are running on the user's computer and are started by the user. When the Vulnerability Monitor component is enabled, you do not need to start the Vulnerability Scan task. This scan is especially relevant when a Vulnerability Scan (see the section "About the Vulnerability Scan task" on page [184](#)) of applications that are installed on the user's computer has not been performed at all or was performed a long time ago.

ENABLING AND DISABLING VULNERABILITY MONITOR

The Vulnerability Monitor component is enabled by default. You can disable Vulnerability Monitor, if necessary.

There are two ways to enable or disable the component:

- On the **Protection and Control** tab of the main application window (see the section "Main application window" on page [46](#))
- From the application settings window (see the section "Application settings window" on page [48](#))

➤ *To enable or disable Vulnerability Monitor on the Protection and Control tab of the main application window:*



1. Open the main application window (on page [46](#)).

2. Select the **Protection and Control** tab.
3. Click the **Endpoint control** section.



The **Endpoint control** section opens.

4. Right-click to display the context menu of the line with information about the Vulnerability Monitor component.
A menu for selecting actions on the component opens.
5. Do one of the following:

- To enable Vulnerability Monitor, select **Enable**.

The component status icon , which is displayed on the left in the **Vulnerability Monitor** line, changes to the icon .

- To disable Vulnerability Monitor, select **Disable**.

The component status icon , which is displayed on the left in the **Vulnerability Monitor** line, changes to the icon .

➤ *To enable or disable Vulnerability Monitor from the application settings window:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Vulnerability Monitor**.
In the right part of the window, the settings of the Vulnerability Monitor component are displayed.
3. In the right part of the window, do one of the following:
 - If you want Kaspersky Endpoint Security to start a vulnerability scan of applications that are running on the user's computer or are started by the user, select the **Enable Vulnerability Monitor** check box.
 - If you do not want Kaspersky Endpoint Security to start a vulnerability scan of applications that are running on the user's computer or are started by the user, clear the **Enable Vulnerability Monitor** check box.
4. To save changes, click the **Save** button.

VIEWING INFORMATION ABOUT VULNERABILITIES OF RUNNING APPLICATIONS

The Vulnerability Monitor component provides information about vulnerabilities in running applications. This information is available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for workstations. This information is not available if Kaspersky Endpoint Security is installed on a computer that runs on Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

➤ *To view information about vulnerabilities of running applications:*

1. Open the main application window (on page [46](#)).
2. Select the **Protection and Control** tab.
3. Click the **Endpoint control** section.

The **Endpoint control** section opens.

4. Click the **Application Activity Monitor** button.

The **Application Activity Monitor** tab in the **Applications** window opens. The **Application Activity Monitor** table shows summary information about the activity of applications that are running in the operating system. The vulnerability status of running applications, as determined by the Vulnerability Monitor component, is shown in the **Vulnerability status** column.

ABOUT THE VULNERABILITY SCAN TASK

Vulnerabilities in the operating system may be caused, for example, by errors in programming or design, weak passwords, or malware activity. When scanning for vulnerabilities, the application analyzes the operating system and searches for anomalies and damaged settings of applications from Microsoft and other vendors.

A vulnerability scan performs operating system security diagnostics and detects software features that can be used by intruders to spread malicious objects and obtain access to personal information.

After the Vulnerability Scan task starts (see the section "Starting or stopping the vulnerability scan task" on page [184](#)), the task progress is displayed in the field that is next to the name of the **Vulnerability Scan** task in the **Tasks** section, on the **Protection and Control** tab of the main window of Kaspersky Endpoint Security.

The results of the vulnerability scan task are logged in reports (see the section "Managing reports" on page [193](#)).

STARTING OR STOPPING THE VULNERABILITY SCAN TASK

Regardless of the run mode that is selected for the Vulnerability Scan task, you can start or stop it at any time.

➤ *To start or stop the Vulnerability Scan task:*

1. Open the main application window (on page [46](#)).
2. Select the **Protection and Control** tab.
3. Click the **Tasks** section.

The **Tasks** section opens.

4. Right-click to display the context menu of the line with the Vulnerability Scan task name.

A menu of actions with the Vulnerability Scan task opens.

5. Do one of the following:

- To start the Vulnerability Scan task, select **Start scanning** from the menu.

The task progress status that is displayed on the right of the button with the name of the Vulnerability Scan task changes to *Running*.

- To stop the Vulnerability Scan task, select **Stop scanning** from the menu.

The task progress status that is displayed on the right of the button with the name of the Vulnerability Scan task changes to *Stopped*.

CREATING THE VULNERABILITY SCAN SCOPE

A vulnerability scan scope is a software vendor or path to the folder to which software has been installed (for example, all Microsoft applications that are installed to the Program Files folder).

➤ *To create a vulnerability scan scope:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Vulnerability Scan**.

In the right part of the window, the Vulnerability Scan task settings are displayed.
3. In the **Objects to scan** section, do one of the following:
 - a. To use Kaspersky Endpoint Security to look for vulnerabilities in Microsoft applications that are installed on the computer, select the **Microsoft** check box.
 - b. To use Kaspersky Endpoint Security to look for vulnerabilities in all applications that are installed on the computer other than those by Microsoft, select the **Other vendors** check box.
 - c. Click the **Additional vulnerability scan scope** button.

The **Vulnerability scan scope** window opens.
 - d. Create the vulnerability scan scope To do so, use the **Add** and **Delete** buttons.
 - e. In the **Vulnerability scan scope** window, click **OK**.
4. To save changes, click the **Save** button.

SELECTING THE VULNERABILITY SCAN TASK RUN MODE

➤ *To select the Vulnerability Scan task run mode:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Vulnerability Scan**.

In the right part of the window, the Vulnerability Scan task settings are displayed.
3. Click the **Run mode** button.

The **Run mode** tab of the **Vulnerability Scan** window opens.

4. In the **Run mode** section, select one of the following run mode options for starting the Vulnerability Scan task:
 - If you want to start the Vulnerability Scan task manually, select **Manually**.
 - If you want to configure a startup schedule for the Vulnerability Scan task, select **By schedule**.
5. Do one of the following:
 - If you have selected the **Manually** option, go to step 6 of these instructions.
 - If you have selected the **By schedule** option, specify the startup settings for the Vulnerability Scan task. To do so:
 - a. In the **Frequency** drop-down list, specify when to start the Vulnerability Scan task. Select one of the following options: **Days**, **Every week**, **At a specified time**, **Every month**, **After application startup**, or **After every update**.
 - b. Depending on the item that is selected in the **Frequency** drop-down list, specify values for the settings that define the startup time of the Vulnerability Scan task.
 - c. If you want Kaspersky Endpoint Security to start skipped Vulnerability Scan tasks as soon as possible, select the **Run skipped tasks** check box

If **After application startup** or **After every update** is selected from the **Frequency** drop-down list, the **Run skipped tasks** check box is unavailable.
 - d. If you want Kaspersky Endpoint Security to suspend the Vulnerability Scan task when computer resources are limited, select the **Suspend scheduled scanning when the screensaver is off and the computer is unlocked** check box. This option for scheduled start of the Vulnerability Scan task helps to conserve the processing capacity of the computer.
6. Click **OK**.
7. To save changes, click the **Save** button.

CONFIGURING THE LAUNCH OF THE VULNERABILITY SCAN TASK UNDER A DIFFERENT USER ACCOUNT

By default, the Vulnerability Scan task is started under the account with which the user is logged into the operating system. However, you may need to start the Vulnerability Scan task under a different user account. You can specify a user who has these rights in the settings of the Vulnerability Scan task and start the Vulnerability Scan task under this user's account.

➤ *To configure the launch of the Vulnerability Scan task under a different user account:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Vulnerability Scan**.
In the right part of the window, the Vulnerability Scan task settings are displayed.
3. Click the **Run mode** button.
The **Run mode** tab of the **Vulnerability Scan** window opens.
4. On the **Run mode** tab, in the **User account** section, select the **Start task as** check box.

5. In the **Name** field, enter the account name of the user whose rights are necessary to start the Vulnerability Scan task.
6. In the **Password** field, enter the password of the user whose rights are necessary to start the Vulnerability Scan task.
7. Click **OK**.
8. To save changes, click the **Save** button.

HANDLING DETECTED VULNERABILITIES

This section contains instructions on managing the list of vulnerabilities that Kaspersky Endpoint Security detects during the Vulnerability Scan task.

IN THIS SECTION:

About vulnerabilities	188
Managing the list of vulnerabilities	189




ABOUT VULNERABILITIES

Kaspersky Endpoint Security logs the results of the Vulnerability Scan task (see the section "About the Vulnerability Scan task" on page [184](#)) in the list of vulnerabilities. This data includes information about the vulnerability source, its importance level, and recommendations on fixing it.

After the user reviews the selected vulnerabilities and performs the actions that are recommended to fix them, Kaspersky Endpoint Security changes the status of the vulnerabilities to *Fixed*.

If the user does not want to display entries about specific vulnerabilities in the vulnerability list, the user may choose to hide these entries. Kaspersky Endpoint Security assigns such vulnerabilities *Hidden* status.

The list of vulnerabilities appears in the form of a table. Each table row contains the following information:

- An icon that signifies the importance level of a vulnerability. Importance levels of detected vulnerabilities have the following types:
 - Icon  **Critical**. This importance level applies to highly dangerous vulnerabilities that must be fixed without delay. Intruders actively exploit vulnerabilities in this group to infect the operating system of computers or to damage user personal data. To eliminate the threat, Kaspersky Lab specialists recommend promptly performing all actions that address vulnerabilities in this group.
 - Icon  **Important**. This importance level applies to important vulnerabilities that need to be fixed soon. No active attempts at exploiting such vulnerabilities are currently detected. Intruders may start exploiting vulnerabilities in this group to infect the operating system of the computer or to damage user personal data. To ensure optimal protection of the computer and personal data of the user, Kaspersky Lab specialists recommend performing actions that address this group of vulnerabilities.
 - Icon  **Warning**. This importance level applies to vulnerabilities for which fixing may be postponed. Intruders are not likely to exploit vulnerabilities in this group at the moment, but these vulnerabilities may threaten the security of the computer in the future.
- Name of application in which the vulnerability is detected.
- Folder that contains the vulnerable file.
- Information about the software publisher, as indicated in the digital signature.
- Decision that Kaspersky Endpoint Security made on how to fix the vulnerability.

MANAGING THE LIST OF VULNERABILITIES

When managing the list of vulnerabilities, you can perform the following actions:

- View the list of vulnerabilities.
- Start the Vulnerability Scan task again after updating databases and application modules.
- View detailed information about the vulnerability and recommendations on fixing it in a separate section.
- Fix the vulnerability.
- Hide selected entries in the list of vulnerabilities.
- Filter the list of vulnerabilities by level of importance.
- Filter the list of vulnerabilities by *Fixed* and *Hidden* status values.

You can also perform the following actions while managing data in the table:

- Filter the list of vulnerabilities by column values or by custom filter conditions.
- Use the vulnerability search function.
- Sort entries in the list of vulnerabilities.
- Change the order and arrangement of columns that are shown in the list of vulnerabilities.
- Group entries in the list of vulnerabilities.

IN THIS SECTION:

Starting the Vulnerability Scan task again	189
Fixing a vulnerability	190
Hiding entries in the list of vulnerabilities	191
Filtering the list of vulnerabilities by importance level	191
Filtering the list of vulnerabilities by Fixed and Hidden status values	192

STARTING THE VULNERABILITY SCAN TASK AGAIN

To rescan previously detected vulnerabilities, you can restart the Vulnerability Scan task. This may be necessary, for example, when the vulnerability scan is interrupted for any reason or if you want Kaspersky Endpoint Security to scan files after the latest database and application module update (see the section "About database and application module updates" on page [159](#)).

➡ *To start the Vulnerability Scan task again:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Vulnerabilities** tab.

The **Vulnerabilities** tab contains a list of vulnerabilities that Kaspersky Endpoint Security has detected during the Vulnerability Scan task.

4. Click the **Rescan** button.

Kaspersky Endpoint Security will rescan all vulnerabilities shown in the list of vulnerabilities.

The status of a vulnerability that has been fixed by the installation of a proposed patch does not change after another vulnerability scan.

FIXING A VULNERABILITY

You can fix a vulnerability by installing an operating system update, changing the application configuration, or installing an application patch.

Detected vulnerabilities may apply not to installed applications but to their copies. A patch can fix a vulnerability only if the application is installed.

➔ *To fix a vulnerability:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Vulnerabilities** tab.

The **Vulnerabilities** tab contains a list of vulnerabilities that Kaspersky Endpoint Security has detected during the Vulnerability Scan task.

4. In the list of vulnerabilities, select the entry that corresponds to the relevant vulnerability.

The **Vulnerability fix** section opens at the bottom of the vulnerability list. The section contains information about this vulnerability and recommendations on how to fix it.

The following information is available for each selected vulnerability:

- Name of application in which the vulnerability is detected.
 - Version of application in which the vulnerability is detected.
 - Severity of the vulnerability.
 - Vulnerability ID.
 - Date and time of last vulnerability detection.
 - Recommendations on fixing the vulnerability (for example, a link to a website with an operating system update or an application patch).
 - Link to a website with a description of the vulnerability.
5. To view a detailed description of the vulnerability, click the **Additional info** link to open a web page with a description of the threat that is associated with the selected vulnerability. The website <http://www.secunia.com> lets you download the necessary update for the current version of the application and install it.
 6. Select one of the following ways to fix a vulnerability:

- If one or more patches are available for the application, install the necessary patch by following the instructions that are provided next to the name of the patch.
- If an operating system update is available, install the necessary update by following the instructions that are provided next to the name of the update.

The vulnerability is fixed after you install the patch or update. Kaspersky Endpoint Security assigns this vulnerability a status that signifies that the vulnerability is fixed. The ✓ icon appears in the line next to the application name. The entry about the fixed vulnerability is shown in gray in the list of vulnerabilities.

7. If no information on how to fix a vulnerability is provided in the **Vulnerability fix** section, you can start the Vulnerability Scan task again after updating Kaspersky Endpoint Security databases and modules. Because Kaspersky Endpoint Security scans the system for vulnerabilities against a database of vulnerabilities, an entry about a fixed vulnerability may appear after the application is updated.

HIDING ENTRIES IN THE LIST OF VULNERABILITIES

You can hide a selected vulnerability entry. Kaspersky Endpoint Security assigns *Hidden* status to entries selected in the list of vulnerabilities and marked as hidden. You can then filter the list of vulnerabilities by the *Hidden* status value (see the section "*Filtering the list of vulnerabilities by Fixed and Hidden status values*" on page [192](#)).

➔ *To hide an entry in the list of vulnerabilities:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Vulnerabilities** tab.

The **Vulnerabilities** tab contains a list of vulnerabilities that Kaspersky Endpoint Security has detected during the Vulnerability Scan task.

4. In the list of vulnerabilities, select the entry that corresponds to the relevant vulnerability.

The **Vulnerability fix** section opens at the bottom of the vulnerability list. The section contains information about this vulnerability and recommendations on how to fix it.

5. Click the **Hide** button.

Kaspersky Endpoint Security assigns *Hidden* status to the selected vulnerability.

When the **Hidden** check box is selected, the selected vulnerability entry is moved to the end of the list of vulnerabilities and shown in gray.

When the **Hidden** check box is cleared, the selected vulnerability entry is not displayed in the list of vulnerabilities.

FILTERING THE LIST OF VULNERABILITIES BY IMPORTANCE LEVEL

➔ *To filter the list of vulnerabilities by importance level:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Vulnerabilities** tab.

The **Vulnerabilities** tab contains a list of vulnerabilities that Kaspersky Endpoint Security has detected during the Vulnerability Scan task.

4. Icons that signify the level of importance of vulnerabilities are displayed next to the **Show importance** setting. Filter the list of vulnerabilities by importance level in one of the following ways:
 - To display vulnerability entries with the corresponding importance level in the list of vulnerabilities, select the necessary icons.
 - To hide vulnerability entries with the corresponding importance level from the list of vulnerabilities, clear the necessary icons.

The list of vulnerabilities shows vulnerability entries with the specified importance level. The specified vulnerability entry filtering conditions are saved after you close the **Reports and Storages** window.

FILTERING THE LIST OF VULNERABILITIES BY FIXED AND HIDDEN STATUS VALUES

➤ *To filter the list of vulnerabilities by Fixed and Hidden status values:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Vulnerabilities** tab.

The **Vulnerabilities** tab contains a list of vulnerabilities that Kaspersky Endpoint Security has detected during the Vulnerability Scan task.

4. Check boxes that signify the status of vulnerabilities are shown next to the **Show vulnerabilities** setting. To filter the list of vulnerabilities by *Fixed* status, do one of the following:
 - To show entries about fixed vulnerabilities in the list of vulnerabilities, select the **Fixed** check box. For entries about fixed vulnerabilities, the ✓ icon is shown next to the application name instead of the icon that signifies the importance level. Entries about fixed vulnerabilities are colored gray in the list of vulnerabilities.
 - To hide entries about fixed vulnerabilities from the list of vulnerabilities, clear the **Fixed** check box.
5. To filter the list of vulnerabilities by *Hidden* status, do one of the following:
 - To display entries about hidden vulnerabilities in the list of vulnerabilities, select the **Hidden** check box. Entries about hidden vulnerabilities are colored gray in the list of vulnerabilities.
 - To hide entries about hidden vulnerabilities from the list of vulnerabilities, clear the **Hidden** check box.

The specified vulnerability entry filtering conditions are not saved after you close the **Reports and Storages** window.

MANAGING REPORTS

This section describes how you can configure report settings and manage reports.

IN THIS SECTION:

Principles of managing reports.....	193
Configuring report settings	194
Generating reports	195
Viewing reported event information in a separate section	196
Saving a report to file	196
Removing information from reports	197

PRINCIPLES OF MANAGING REPORTS




Information about the operation of each Kaspersky Endpoint Security component, performance of each scan task, update task, and vulnerability scan task, and operation of the application overall is recorded in the report.

Report data is presented in the form of a table which contains a list of events. Each table line contains information on a separate event. Event attributes are located in the table columns. Certain columns are compound ones which contain nested columns with additional attributes. Events that are logged during the operation of various components and tasks have different sets of attributes.

You can generate reports of the following types:

- **System Audit report.** Contains information about events occurring during the interaction between the user and the application and in the course of application operation in general, which are unrelated to any particular Kaspersky Endpoint Security component or task.
- **All protection components report.** Contains information about events that are logged in the course of operation of the following Kaspersky Endpoint Security components:
 - File Anti-Virus
 - Mail Anti-Virus
 - Web Anti-Virus
 - IM Anti-Virus
 - System Watcher
 - Firewall
 - Network Attack Blocker
- Report on the operation of a Kaspersky Endpoint Security component or task. Contains information about events that occur in the course of operation of a selected Kaspersky Endpoint Security component or task.

Event importance levels are of the following types:

- Icon . **Informative events.** Formal events that do not normally contain important information.
- Icon . **Important events.** Events that need attention because they reflect important situations in the operation of Kaspersky Endpoint Security.
- Icon . **Critical events.** Events of critical importance and faults that indicate problems in the operation of Kaspersky Endpoint Security or vulnerabilities in protection of the user's computer.

For convenient processing of reports, you can modify the presentation of data on the screen in the following ways:

- Filter the event list by various criteria.
- Use the search function to find a specific event.
- View the selected event in a separate section.
- Sort the list of events by each column.
- Maximize or minimize grouped data.
- Change the order and arrangement of columns that are shown in the report.

You can save a generated report to a text file, if necessary.

You can also delete report information on Kaspersky Endpoint Security components and tasks that are combined into groups. Kaspersky Endpoint Security deletes all entries of the selected reports from the earliest entry until the time of deletion.

CONFIGURING REPORT SETTINGS

You can configure report settings in the following ways:

- Configure the maximum report storage term.

The default maximum storage term for reports on events that are logged by Kaspersky Endpoint Security is 30 days. After that period of time, Kaspersky Endpoint Security automatically deletes the oldest entries from the report file. You can cancel the time-based restriction or change the maximum report storage duration.

- Configure the maximum size of the report file.

You can specify the maximum size of the file that contains the report. By default, the maximum report 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. You can cancel the restriction on the size of the report file or set a different value.

IN THIS SECTION:

Configuring the maximum report storage term	195
Configuring the maximum size of the report file	195

CONFIGURING THE MAXIMUM REPORT STORAGE TERM

➔ *To modify the report maximum storage term:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Reports and Storages**.
3. In the right part of the window, in the **Report settings** section, perform one of the following:
 - To limit the report storage term, select the **Store reports no longer than** check box. In the field next to the **Store reports no longer than** check box, specify the maximum report storage term. The default maximum storage term for reports is 30 days.
 - To cancel the limit on the report storage term, clear the **Store reports no longer than** button.

The limit on the report storage term is enabled by default.

4. To save changes, click the **Save** button.

CONFIGURING THE MAXIMUM SIZE OF THE REPORT FILE

➔ *To configure the maximum report file size:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Reports and Storages**.
3. In the right part of the window, in the **Report settings** section, do one of the following:
 - To limit the report file size, select the **Maximum file size** check box. In the field on the right of the **Maximum file size** check box, specify the maximum report file size. By default, the report file size is limited to 1024 MB.
 - To remove the restriction on the report file size, clear the **Maximum file size** check box.

The report file size limit is enabled by default.

4. To save changes, click the **Save** button.

GENERATING REPORTS

➔ *To generate reports:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

The **Reports** tab of the **Reports and Storages** window opens.

The System Audit report is displayed under the **Reports** tab by default.

3. To generate the All Protection Components report, in the left part of the **Reports and Storages** window, select the **All protection components** item in the list of components and tasks.

The All Protection Components report is displayed in the right part of the window, which contains a list of events in the operation of all protection components of Kaspersky Endpoint Security.

- To generate a report on the operation of a component or task, in the left part of the **Reports and Storages** window, in the list of components and tasks, select a component or task.

A report is displayed in the right part of the window, which contains a list of events in the operation of the selected Kaspersky Endpoint Security component or task.

By default, report events are sorted in the ascending order of values in the **Event date** column.

VIEWING REPORTED EVENT INFORMATION IN A SEPARATE SECTION

You can view logged event details in a separate section.

➤ *To view event details in a separate section:*

- Open the main application window (on page [46](#)).
- In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.

The **Reports** tab of the **Reports and Storages** window opens.

The System Audit report is displayed under the **Reports** tab by default. This report contains information about events that are logged as the application operates and interacts with the user.

- Do one of the following:

- To generate a general protection report, select the **All Protection Components** item in the list of components and tasks.

The "All protection components" report is displayed in the right part of the window, containing a list of events in the operation of all protection components.

- To generate a report on the operation of a specific component or task, select this component or task in the list of components and tasks.

A report is displayed in the right part of the window, containing a list of events in the operation of the selected component or task.

- If necessary, use the filter, search, and sorting functions to locate the necessary event in the report.
- Select the found event in the report.

A section appears in the lower part of the window, with the attributes of this event and information about its importance level.

SAVING A REPORT TO FILE

You can save the report that you generate to a file in text format (TXT) or a CSV file.

Kaspersky Endpoint Security logs events in the report such as they are displayed on the screen: in other words, with the same set and sequence of event attributes.

➤ *To save a report to file:*

- Open the main application window (on page [46](#)).

- In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.

The **Reports** tab of the **Reports and Storages** window opens.

The System Audit report is displayed under the **Reports** tab by default. This report contains information about events that are logged as the application operates and interacts with the user.

- Do one of the following:
 - To generate the "All protection components" report, select **All protection components** in the list of components and tasks.

The "All protection components" report is displayed in the right part of the window, containing a list of events in the operation of all protection components.
 - To generate a report on the operation of a specific component or task, select this component or task in the list of components and tasks.

A report is displayed in the right part of the window, containing a list of events in the operation of the selected component or task.

- If necessary, you can modify data presentation in the report by:
 - Filtering events
 - Running an event search
 - Rearranging columns
 - Sorting events

- Click the **Save report** button in the upper right part of the window.

A context menu opens.

- In the context menu, select the encoding for saving the report file: **Save in ANSI** or **Save in Unicode**.

The standard **Save as** window of Microsoft Office opens.

- In the **Save as** window, specify the destination folder for the report file.

- In the **File name** field, type the report file name.

- In the **File type** field, select the necessary report file format: TXT or CSV.

- Click the **Save** button.

REMOVING INFORMATION FROM REPORTS

➔ *To remove information from reports:*

- Open the application settings window (on page [48](#)).
- In the left part of the window, in the **Advanced Settings** section, select **Reports and Storages**.
- In the right part of the window, in the **Report settings** section, click the **Clear reports** button.

The **Clearing reports** window opens.

4. Select check boxes opposite the reports from which you want to delete information:
 - **All reports.**
 - **General protection report.** Contains information about the operation of the following Kaspersky Endpoint Security components:
 - File Anti-Virus
 - Mail Anti-Virus
 - Web Anti-Virus
 - IM Anti-Virus
 - Firewall
 - Network Attack Blocker
 - **Scan tasks report.** Contains information about completed scan tasks:
 - Full Scan.
 - Critical Areas Scan.
 - Custom Scan.
 - **Update task report.** Contains information about completed update tasks:
 - **Firewall rules processing report.** Contains information about Firewall operation.
 - **Control components report.** Contains information about the operation of the following Kaspersky Endpoint Security components:
 - Application Startup Control
 - Application Privilege Control
 - Vulnerability Monitor
 - Device Control
 - Web Control
 - **Data from System Watcher.** Contains information about System Watcher operation.
5. Click **OK**.

NOTIFICATION SERVICE

This section describes the service of notifications alerting the user to events in the operation of Kaspersky Endpoint Security and contains instructions on configuring the delivery of notifications.

IN THIS SECTION:

About Kaspersky Endpoint Security notifications	199
Configuring the notification service	199
Viewing Microsoft Windows Event Log.....	201

ABOUT KASPERSKY ENDPOINT SECURITY NOTIFICATIONS

All sorts of events occur during the operation of Kaspersky Endpoint Security. They can be either formal or critical. Examples of events range from reports on a successful database and application module update to component errors that need remedying.

Kaspersky Endpoint Security supports the logging of information about events in the operation of the application in the event log of Microsoft Windows and / or the event log of Kaspersky Endpoint Security.

Kaspersky Endpoint Security delivers notifications in one of the following ways:

- Displays notifications on the screen as pop-up messages in the Microsoft Windows taskbar notification area.
- Delivers notifications by email.

You can configure the delivery of event notifications. The method of notification delivery is configured for each type of event.

CONFIGURING THE NOTIFICATION SERVICE

You can configure the notification service in the following ways:

- Configure the settings of event logs where Kaspersky Endpoint Security records events.
- Configure the delivery of on-screen notifications.
- Configure the delivery of email notifications.

When using the table of events to configure the notification service, you can do the following:

- Filter notification service events by column values or by custom filter conditions.
- Use the search function for notification service events.
- Sort notification service events.
- Change the order and set of columns that are displayed in the list of notification service events.

IN THIS SECTION:

Configuring event log settings	200
Configuring delivery of on-screen and email notifications	200

CONFIGURING EVENT LOG SETTINGS

➔ *To configure event log settings:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Interface**.
The user interface settings are displayed in the right part of the window.
3. In the **Notifications** section, click the **Settings** button.
4. The **Notifications** window opens.
Kaspersky Endpoint Security components and tasks are shown in the left part of the window. The right part of the window lists events generated for the selected component or task.
5. In the left part of the window, select the component or task for which you want to configure the event log settings.
6. Select check boxes opposite the relevant events in the **Save locally** and **Save in Windows Event Log** columns.
Events in the **Save in local log** column are logged in the Kaspersky Endpoint Security Event Log. Events in the **Save in Windows Event Log** column are logged in the Microsoft Windows event log.
7. Click **OK**.
8. To save changes, click the **Save** button.

CONFIGURING DELIVERY OF ON-SCREEN AND EMAIL NOTIFICATIONS

➔ *To configure delivery of on-screen and email notifications:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Interface**.
The user interface settings are displayed in the right part of the window.
3. In the **Notifications** section, click the **Settings** button.
4. The **Notifications** window opens.
Kaspersky Endpoint Security components and tasks are shown in the left part of the window. The right part of the window lists events generated for the selected component or task.
5. In the left part of the window, select the component or task for which you want to configure the delivery of notifications.
6. In the **Notify on screen** column, select the check boxes next to the required events.

Information about the selected events is displayed on the screen as pop-up messages in the Microsoft Windows taskbar notification area.

7. In the **Notify by email** column, select the check boxes next to the required events.

Information about the selected events is delivered by email.

8. Click the **Email notification settings** button.

The **Email notification settings** window opens.

9. Select the **Enable email notifications about events** check box to enable the delivery of notifications about Kaspersky Endpoint Security events selected in the **Notify by email** column.

10. Specify the email notification delivery settings.

11. Click **OK**.

12. In the **Email notification settings** window, click **OK**.

13. To save changes, click the **Save** button.

VIEWING MICROSOFT WINDOWS EVENT LOG

➤ *To view the Microsoft Windows event log,*

select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Event Viewer**.

MANAGING QUARANTINE AND BACKUP

This section describes how you can configure and manage Quarantine and Backup.

IN THIS SECTION:

About Quarantine and Backup	202
Configuring Quarantine and Backup settings	203
Managing Quarantine.....	204
Managing Backup	208

ABOUT QUARANTINE AND BACKUP

Quarantine is a list of files that are probably infected with viruses and other malware. *Probably infected files* are files that are suspected of being infected with viruses and other malware or their modifications.

When Kaspersky Endpoint Security quarantines a probably infected file, it does not copy the file, but moves it: the application deletes the file from the hard drive or email message and saves the file in a special data storage. Files in Quarantine are saved in a special format and do not pose a threat.

Kaspersky Endpoint Security can detect and quarantine a probably infected file when scanning for viruses and other threats (see the section "Scanning the computer" on page [168](#)), and during the operation of File Anti-Virus (see the section "About File Anti-Virus" on page [51](#)), Mail Anti-Virus (see the section "About Mail Anti-Virus" on page [64](#)) and System Watcher (on page [61](#)).

Kaspersky Endpoint Security places files in Quarantine in the following cases:

- File code resembles a known but partly modified threat, or has a malware-like structure, but is not listed in the Kaspersky Endpoint Security database. In this case, the file is placed in Quarantine after heuristic analysis by File Anti-Virus and Mail Anti-Virus, or during scanning for viruses and other threats. Heuristic analysis rarely causes false positives.
- The sequence of operations that a file performs raises suspicions. In this case, the file is placed in Quarantine after the System Watcher component has analyzed its behavior.

You can also manually place a file that you suspect of containing viruses or other malware in Quarantine.

Backup storage is a list of backup copies of files that have been deleted or modified during the disinfection process. *Backup copy* is a copy of the file, which is created at the first attempt to disinfect or delete this file and is stored in the same storage as potentially infected files. Backup copies of files are stored in a special format and do not pose a threat.

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

It is possible that, after another database or application software module update, Kaspersky Endpoint Security may be able to definitively identify the threat and neutralize it. It is therefore recommended to scan quarantined files after each database and application software module update.

File status may change after quarantined files are scanned with updated threat signatures:

- If a file cannot be disinfected during scanning, the file status *Infected* remains the same.
- If a file is disinfected during scanning, the status *Not infected* is assigned to this file. You can restore this file to its original folder.

CONFIGURING QUARANTINE AND BACKUP SETTINGS

Data storage consists of Quarantine and Backup. You can configure Quarantine and Backup settings as follows:

- Configure the maximum storage term for files in Quarantine and file copies in Backup.

The default maximum storage term for files in Quarantine and file copies in Backup is 30 days. When the maximum storage term expires, Kaspersky Endpoint Security deletes the oldest files from the data storage. You can cancel the time-based restriction or change the maximum file storage term.

- You can configure the maximum Quarantine and Backup size.

By default, the maximum Quarantine and Backup size is 100 MB. When data storage reaches its limit, Kaspersky Endpoint Security automatically deletes the oldest files from Quarantine and Backup so that the maximum data storage size is not exceeded. You can cancel the Quarantine and Backup size limit or change their maximum size.

IN THIS SECTION:

Configuring the maximum storage term for files in Quarantine and file copies in Backup [203](#)

Configuring the maximum size of Quarantine and Backup..... [204](#)

CONFIGURING THE MAXIMUM STORAGE TERM FOR FILES IN QUARANTINE AND FILE COPIES IN BACKUP

➔ *To configure the maximum storage term for files in Quarantine and file copies in Backup:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Reports and Storages**.
3. Do one of the following:
 - To limit the Quarantine and Backup file storage term, in the right part of the window, in the **Local quarantine and backup settings** section, select the **Store objects no longer than** check box. In the field on the right of the **Store objects no longer than** check box, specify the maximum storage term for files in Quarantine and file copies in Backup. The storage term for files in Quarantine and file copies in Backup is limited to 30 days by default.
 - To cancel the Quarantine and Backup file storage term limitation, in the right part of the window, in the **Local quarantine and backup settings** section, select the **Store objects no longer than** check box.
4. To save changes, click the **Save** button.

CONFIGURING THE MAXIMUM SIZE OF QUARANTINE AND BACKUP

➤ *To configure the maximum Quarantine and Backup size:*

1. Open the application settings window (on page [48](#)).
 2. In the left part of the window, in the **Advanced Settings** section, select **Reports and Storages**.
 3. Do one of the following:
 - To limit the size of Quarantine and Backup, in the right part of the window, in the **Local quarantine and backup settings** section, select the **Maximum size** check box. In the field on the right of the **Maximum size** check box, specify the maximum size of Quarantine and Backup. By default, the maximum size is 100 MB.
 - To cancel the data storage size limit, in the right part of the window, in the **Local quarantine and backup settings** section, clear the **Maximum size** check box.
- The Quarantine and Backup size limit is disabled by default.
4. To save changes, click the **Save** button.

MANAGING QUARANTINE

The following file operations are available when managing Quarantine:

- View the list of files that are quarantined by Kaspersky Endpoint Security.
- Manually move to Quarantine files that you suspect of posing a threat.
- Scan potentially infected files by using the current version of Kaspersky Endpoint Security databases and modules.
- Restore files from Quarantine to their original folders.
- Remove files from Quarantine.
- Open the folder where a file was located originally.
- Send potentially infected files to Kaspersky Lab for examination.

The list of quarantined files is displayed in table form. Each table row contains an event with information about the potentially infected file (this is called a "Quarantine event") and the type of threat that has been detected.

You can also perform the following actions while managing data in the table:

- Filter Quarantine events by column value or by using custom filter conditions.
- Use the Quarantine event search function.
- Sort Quarantine events.
- Change the order and set of columns that are displayed in the list of Quarantine events.
- Group Quarantine events.

You can copy selected Quarantine events to the clipboard, if necessary.

IN THIS SECTION:

Moving a file to Quarantine	205
Starting a Custom Scan task for files in Quarantine	206
Restoring files from Quarantine	206
Deleting files from Quarantine	207
Sending potentially infected files to Kaspersky Lab for examination	207

MOVING A FILE TO QUARANTINE

Kaspersky Endpoint Security automatically quarantines potentially infected files that are detected by the protection components or during a computer scan for viruses and other threats.

You can manually quarantine files that you suspect of containing viruses or other threats.

You can place files in Quarantine in two ways:

- By clicking the **Move to Quarantine** button, on the **Quarantine** tab of the **Reports and Storages** window.
- By using the context menu that is opened in the standard **My Documents** window of Microsoft Windows.

➤ *To quarantine a file from the Quarantine tab of the Reports and Storages window:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

The **Quarantine** tab of the **Reports and Storages** window opens.

The **Quarantine** tab contains a list of potentially infected files that Kaspersky Endpoint Security has detected while scanning the computer.

3. Click the **Move to Quarantine** button.
4. The standard **Open file** window in Microsoft Windows opens.
5. Select the file that you want to move to Quarantine.
6. Click the **Open** button.

The selected file appears in the table on the **Quarantine** tab. Access to this file is blocked. The file is moved from its original folder to Quarantine. The file is saved in Quarantine in encrypted form, which prevents it from infecting the operating system.

➤ *To move a file to Quarantine from the My Documents window in Microsoft Windows:*

1. Double-click the **My Documents** shortcut on the desktop of the operating system.

The standard **My Documents** window opens in Microsoft Windows.

2. Go to the folder that contains the file that you want to move to Quarantine.
3. Select the file that you want to move to Quarantine.

4. Right-click to display the context menu of the file.
5. In the context menu, select **Move to Quarantine**.

Access to the file is blocked. The file is moved to Quarantine from its original folder. The file is saved in Quarantine in encrypted form, which prevents it from infecting the operating system.

STARTING A CUSTOM SCAN TASK FOR FILES IN QUARANTINE

After an update of databases and application software modules, Kaspersky Endpoint Security may be able to identify definitively the type of threat that is posed by quarantined files and neutralize it. If the application is not configured to scan quarantined files automatically after each update of databases and application software modules, you can manually start a Custom Scan task for quarantined files.

➤ *To start a Custom Scan task for quarantined files:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

The **Quarantine** tab of the **Reports and Storages** window opens.

3. On the **Quarantine** tab, select one or more Quarantine events that involve potentially infected files that you want to scan. To select multiple Quarantine events, select them while holding down the **CTRL** key.
4. Start the Custom Scan task in one of the following ways:
 - Click the **Rescan** button.
 - Right-click to display the context menu. Select **Rescan**.

When the scan is completed, a notification with the number of scanned files and the number of detected threats appears.

RESTORING FILES FROM QUARANTINE

➤ *To restore files from Quarantine:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

The **Quarantine** tab of the **Reports and Storages** window opens.

3. To restore all quarantined files:
 - a. Right-click anywhere in the table on the **Quarantine** tab to display the context menu.
 - b. Select **Restore all**.

Kaspersky Endpoint Security restores all files from Quarantine to their original folders.

4. To restore one or more quarantined files:
 - a. On the **Quarantine** tab, select one or more Quarantine events that involve files that you want to restore from Quarantine. To select multiple Quarantine events, select them while holding down the **CTRL** key.
 - b. Restore files in one of the following ways:

- Click the **Restore** button.
- Right-click to display the context menu. Select **Restore**.

Kaspersky Endpoint Security restores the selected files to their original folders.

DELETING FILES FROM QUARANTINE

You can delete a quarantined file. Before deleting the quarantined file, Kaspersky Endpoint Security creates a backup copy of the file and saves it in Backup in case you need to later restore the file (see the section "Restoring files from Backup" on page [208](#)).

➤ *To delete files from Quarantine:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

The **Quarantine** tab of the **Reports and Storages** window opens.

3. On the **Quarantine** tab, select one or more Quarantine events that involve potentially infected files that you want to delete from Quarantine. To select multiple Quarantine events, select them while holding down the **CTRL** key.
4. Delete files in one of the following ways:
 - Click the **Delete** button.
 - Right-click to display the context menu. Select **Delete**.

Kaspersky Endpoint Security deletes the selected files from Quarantine. Kaspersky Endpoint Security creates a backup copy of each file and saves the copy in Backup.

SENDING PROBABLY INFECTED FILES TO KASPERSKY LAB FOR EXAMINATION

You must have an email client and a configured Internet connection to be able to send probably infected files to Kaspersky Lab.

➤ *To send a probably infected file to Kaspersky Lab for examination:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

The **Quarantine** tab of the **Reports and Storages** window opens.

3. On the **Quarantine** tab, select one or more Quarantine events that involve potentially infected files that you want to send to Kaspersky Lab for examination. To select multiple Quarantine events, select them while holding down the **CTRL** key.
4. Right-click to display the context menu.
5. Select **Send to Kaspersky Lab**.

An email message window opens in the email client that is installed on your computer. The email message contains an archive with the files that you are sending, the recipient address newvirus@kaspersky.com, and the subject line "Quarantined object".

MANAGING BACKUP

If malicious code is detected in the file, Kaspersky Endpoint Security blocks the file, removes it from its original folder, places its copy in Backup, and attempts to disinfect it. If file disinfection succeeds, the status of the backup copy of the file changes to *Disinfected*. You can restore the file from its disinfected backup copy to its original folder.

Kaspersky Endpoint Security automatically deletes backup copies of files with any status from Backup after the storage term configured in the advanced settings has elapsed.

You can also manually delete the backup copy of either a restored or unrestored file.

The list of backup copies of files appears in the form of a table. Each table row contains an event that involves an infected file (also called a "Backup event") and specifies the type of threat that is detected in the file.

While managing Backup, you can perform the following actions with backup copies of files:

- View the list of backup copies of files.
- Restore files from backup copies to their original folders.
- Delete backup copies of files from Backup.

You can also perform the following actions while managing data in the table:

- Filter Backup events by column value or custom filter conditions.
- Use the Backup event search function.
- Sort Backup events.
- Group Backup events.
- Change the order and set of columns that are displayed in the list of Backup events.

You can copy selected Backup events to the clipboard, if necessary.

IN THIS SECTION:

Restoring files from Backup	208
Deleting backup copies of files from Backup	209

RESTORING FILES FROM BACKUP

We recommend that you restore files from backup copies only when they have *Disinfected* status.

➤ *To restore files from Backup:*

1. Open the main application window (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.

3. In the **Reports and Storages** window, select the **Backup** tab.
4. To restore all files from Backup:
 - a. Right-click anywhere in the table on the **Backup** tab to display the context menu.
 - b. Select **Restore all**.

Kaspersky Endpoint Security restores all files from their backup copies to their original folders.

5. To restore one or more files from Backup :
 - a. In the table, on the **Backup** tab, select one or more Backup events. To select multiple events, select them while holding down the **CTRL** key.
 - b. Click the **Restore** button.

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 (on page [46](#)).
2. In the upper part of the main application window, click the **Quarantine** link to open the **Reports and Storages** window.
3. In the **Reports and Storages** window, select the **Backup** tab.
4. On the **Backup** tab, select one or more Backup events. To select multiple Backup events, select them while holding down the **CTRL** key.
5. Click the **Delete** button.

ADVANCED APPLICATION SETTINGS

This section describes advanced settings of Kaspersky Endpoint Security and how they can be configured.

IN THIS SECTION:

Trusted zone	210
Kaspersky Endpoint Security Self-Defense.....	217
Performance of Kaspersky Endpoint Security and compatibility with other applications	219
Password protection.....	223

TRUSTED ZONE

This section contains information on the trusted zone and instructions on configuring exclusion rules and creating a list of trusted applications.

IN THIS SECTION:

About the trusted zone	210
Configuring the trusted zone	212

ABOUT THE TRUSTED ZONE

A *trusted zone* is a system administrator-configured 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.

The administrator forms the trusted zone independently, taking into account the features of the objects that are handled and the applications that are installed on the computer. It may be necessary to include objects and applications in the trusted zone when Kaspersky Endpoint Security blocks access to a certain object or application, if you are sure that the object or application is harmless.

You can exclude objects of the following types from scanning:

- Files of certain formats
- Files that are selected by a mask
- A certain scope (such as a folder or application)
- Application processes
- Objects that are classified according to the Kaspersky Lab Virus Encyclopedia (depending on the status that is assigned to them by Kaspersky Endpoint Security during scanning).

Exclusion rule

An *exclusion rule* is a set of conditions upon which Kaspersky Endpoint Security does not scan an object for viruses or other threats.

Threat type is the status that Kaspersky Endpoint Security assigns to an object during scanning for viruses and other threats. The status is assigned based on the classification of malware and other programs that are listed in the Kaspersky Lab Virus Encyclopedia. Clicking the link <http://www.securelist.com/en/descriptions> takes you to the website of the Kaspersky Lab Virus Encyclopedia, which contains details of the threat that is associated with the object.

In turn, exclusion rules make it possible to safely use legitimate applications that can be exploited by intruders to harm the computer or user data. Although they do not have any malicious functions, such applications can be used as an auxiliary component in malware. Examples of such applications include remote administration tools, IRC clients, FTP servers, various utilities for suspending or concealing processes, keyloggers, password crackers, and auto-dialers. While not classified as viruses (not-a-virus), these applications can be put in the same class with such programs as Adware or Riskware. Details on adware and legitimate software that criminals can use to damage your computer or personal data are available on the website of the Kaspersky Lab Virus Encyclopedia at <http://www.securelist.com/en/threats/detect>.

Such applications may be blocked by Kaspersky Endpoint Security. To prevent them from being blocked, you can configure rules that exclude them from Kaspersky Endpoint Security scanning. To do so, add the name or mask of the threat that is listed in the Kaspersky Lab Virus Encyclopedia to the trusted zone. For example, you may frequently use the Remote Administrator program. This is a remote access application that gives you control over a remote computer. Kaspersky Endpoint Security regards this activity as potentially dangerous and may block it. To prevent the application from being blocked, create an exclusion rule that specifies Remote Administrator as the threat type.

Exclusion rules can be used by the following application components and tasks that are specified by the system administrator:

- File Anti-Virus
- Mail Anti-Virus
- Web Anti-Virus
- Application Privilege Control
- Scan tasks
- System Watcher

List of trusted applications

The *list of trusted applications* is a list of applications whose file and network activity (including suspicious activity) and access to the system registry are not monitored by Kaspersky Endpoint Security. By default, Kaspersky Endpoint Security scans objects that are opened, executed, or saved by any program process and controls the activity of all applications and network traffic that is generated by them. Kaspersky Endpoint Security excludes applications in the list of trusted applications from scanning (see the section "Editing the list of trusted applications" on page [215](#)).

For example, if you consider objects that are used by the standard Microsoft Windows Notepad application to be safe without scanning, meaning that you trust this application, you can add Microsoft Windows Notepad to the list of trusted applications. Scanning then skips objects that are used by this application.

In addition, certain actions that are classified by Kaspersky Endpoint Security as dangerous may be safe within the context of the functionality of a number of applications. For example, the interception of text that is typed from the keyboard is a routine process for automatic keyboard layout switchers (such as Punto Switcher). To take account of the specifics of such applications and exclude their activity from monitoring, we recommend that you add such applications to the trusted applications list.

Excluding trusted applications from scanning allows avoiding compatibility conflicts between Kaspersky Endpoint Security and other programs (for example, the problem of double-scanning of the network traffic of a third-party computer by Kaspersky Endpoint Security and by another anti-virus application), and also increases the computer's performance, which is critical when using server applications.

At the same time, the executable file and process of the trusted application are still scanned for viruses and other malware. An application can be fully excluded from Kaspersky Endpoint Security scanning by means of exclusion rules.

CONFIGURING THE TRUSTED ZONE

You can configure the trusted zone in the following ways:

- Create a new exclusion rule.

You can create a new exclusion rule whereby Kaspersky Endpoint Security skips the scanning of a specified object or threat type.

- Suspend an exclusion rule.

You can temporarily suspend an exclusion rule without deleting it from the list of exclusion rules.

- Edit the settings of an existing exclusion rule.

After you create a new exclusion rule, you can always return to editing its settings and modify them as needed.

- Delete an exclusion rule.

You can delete an exclusion rule to stop Kaspersky Endpoint Security from using it while scanning the computer.

- Create a list of trusted applications.

You can create a list of applications for which Kaspersky Endpoint Security does not monitor file and network activity (including suspicious activity) and access to the system registry.

- Suspend the exclusion of a trusted application from Kaspersky Endpoint Security scanning.

You can temporarily suspend the exclusion of a trusted application from Kaspersky Endpoint Security scanning without removing the application from the list of trusted applications.

IN THIS SECTION:

Creating an exclusion rule.....	212
Editing an exclusion rule	214
Removing an exclusion rule	214
Starting or stopping an exclusion rule	215
Editing the list of trusted applications	215
Including or excluding a trusted application from scanning	216

CREATING AN EXCLUSION RULE

Kaspersky Endpoint Security does not scan an object when a hard drive or folder that contains this object is specified at the start of a scan task. However, the exclusion rule is not applied when a custom scan task is started for this particular object.

➤ *To create an exclusion rule:*

1. Open the application settings window (on page [48](#)).

2. In the left part of the window, select the **Anti-Virus protection** section.

The anti-virus protection settings are shown in the right part of the window.

3. In the **Exclusions and trusted applications** section, click the **Settings** button.

The **Trusted zone** window opens on the **Exclusion rules** tab.

4. Click the **Add** button.

The **Exclusion rule** window opens.

5. To exclude a file or folder from Kaspersky Endpoint Security scanning:

a. In the **Properties** section, select the **Object** check box.

b. Click the **select object** link in the **Rule description** section. Open the **Object name** window. In this window, you can specify the file or folder name or the mask of the object name, or select the object in the Microsoft Windows folder tree.

c. After selecting the object, in the **Object name** window, click **OK**.

A link to the added object appears in the **Exclusion rule** window, in the **Rule description** section.

6. To exclude objects by specific threat type from Kaspersky Endpoint Security scanning:

a. In the **Properties** section, select the **Threat type** check box.

Threat type is the status that Kaspersky Endpoint Security assigns to an object during scanning for viruses and other threats. The status is assigned based on the classification of malware and other programs that are listed in the Kaspersky Lab Virus Encyclopedia.

b. Click the **enter threat name** link in the **Rule description** section. Open the **Threat type** window. In this window, you can enter the threat type name or mask of the threat type name according to the classification of the Kaspersky Lab Virus Encyclopedia.

c. In the **Threat type** window, click **OK**.

7. In the **Comment** field, enter a brief description of the exclusion rule that you are creating.

8. Specify the Kaspersky Endpoint Security components that should use the exclusion rule:

a. Click the **any** link in the **Rule description** section to open the **select components** link.

b. Clicking the **select components** link to open the **Protection components** window. In this window you can select the relevant components.

c. In the **Protection components** window, click **OK**.

If the components are specified in the settings of the exclusion rule, the object is not scanned only by these components of Kaspersky Endpoint Security.

If the components are not specified in the settings of the exclusion rule, the object is not scanned by all components of Kaspersky Endpoint Security.

9. In the **Exception rule** window, click **OK**.

The added exclusion rule appears in the list of exclusion rules on the **Exclusion rules** tab of the **Trusted zone** window. The configured settings of this exclusion rule are displayed in the **Rule description** section.

10. In the **Trusted zone** window, click **OK**.
11. To save changes, click the **Save** button.

EDITING AN EXCLUSION RULE

➤ *To edit an exclusion rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens on the **Exclusion rules** tab.
4. In the list of exclusion rules, select the necessary exclusion rule.
5. Click the **Edit** button.
The **Exclusion rule** window opens.
6. Edit the settings of an exclusion rule.
7. In the **Exception rule** window, click **OK**.
The edited settings of this exclusion rule are displayed in the **Rule description** section.
8. In the **Trusted zone** window, click **OK**.
9. To save changes, click the **Save** button.

REMOVING AN EXCLUSION RULE

➤ *To delete an exclusion rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens on the **Exclusion rules** tab.
4. In the list of exclusion rules, select the necessary exclusion rule.
5. Click the **Delete** button.
The deleted exclusion rule disappears from the list of exclusion rules.
6. In the **Trusted zone** window, click **OK**.
7. To save changes, click the **Save** button.

STARTING OR STOPPING AN EXCLUSION RULE

➤ *To start or stop an exclusion rule:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens on the **Exclusion rules** tab.
4. In the list of exclusion rules, select the necessary exclusion rule.
5. Do one of the following:
 - To enable this exclusion rule, select the check box next to the name of the exclusion rule.
 - To disable this exclusion rule, clear the check box next to the name of this exclusion rule.
6. Click **OK**.
7. To save changes, click the **Save** button.

EDITING THE LIST OF TRUSTED APPLICATIONS

➤ *To edit the list of trusted applications:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens.
4. In the **Trusted zone** window, select the **Trusted applications** tab.
5. To add an application to the trusted applications list:
 - a. Click the **Add** button.
 - b. In the context menu that opens, do one of the following:
 - To find the application in the list of applications that are installed on the computer, select the **Applications** item in the menu. The **Select application** window opens.
 - To specify the path to the executable file of the relevant application, select **Browse**. The standard **Open file** window in Microsoft Windows opens.

These actions cause the **Exclusions for application** window to open.

- c. Select check boxes opposite the kinds of application activity that you want to skip during scanning:
 - **Do not scan opened files.**

- Do not monitor application activity.
 - Do not inherit restrictions of the parent process (application).
 - Do not monitor child application activity.
 - Allow interaction with application interface.
 - Do not scan network traffic.
- d. In the **Exclusions for application** window, click **OK**.
- The trusted application that you have added appears in the trusted applications list.
6. To edit the settings of a trusted application:
- a. Select a trusted application in the trusted applications list.
 - b. Click the **Edit** button.
 - c. The **Exclusions for application** window opens.
 - d. Change the status of check boxes that are opposite the relevant kinds of application activity.
- If no kind of activity is selected in the **Exclusions for application** window, the trusted application is included in scanning (see the section "Including or excluding a trusted application from scanning" on page [216](#)). In this case the trusted application is not removed from the list of trusted applications, but its check box is cleared.
- e. In the **Exclusions for application** window, click **OK**.
7. To remove a trusted application from the trusted applications list:
- a. Select a trusted application in the trusted applications list.
 - b. Click the **Delete** button.
8. In the **Trusted zone** window, click **OK**.
9. To save changes, click the **Save** button.

INCLUDING OR EXCLUDING A TRUSTED APPLICATION FROM SCANNING

➤ *To include or exclude a trusted application from scanning:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the **Exclusions and trusted applications** section, click the **Settings** button.
The **Trusted zone** window opens.
4. In the **Trusted zone** window, select the **Trusted applications** tab.
5. In the list of trusted applications, select the necessary trusted application.
6. Do one of the following:

- To exclude a trusted application from Kaspersky Endpoint Security scanning, select the check box next to its name.
 - To include a trusted application in Kaspersky Endpoint Security scanning, clear the check box next to its name.
7. Click **OK**.
 8. To save changes, click the **Save** button.

KASPERSKY ENDPOINT SECURITY SELF-DEFENSE

This section describes the self-defense and remote control defense mechanisms of Kaspersky Endpoint Security and provides instructions on configuring the settings of these mechanisms.

IN THIS SECTION:

About Kaspersky Endpoint Security Self-Defense	217
Enabling or disabling Self-Defense	217
Enabling or disabling Remote Control Defense.....	218
Supporting remote administration applications.....	218

ABOUT KASPERSKY ENDPOINT SECURITY SELF-DEFENSE

Kaspersky Endpoint Security protects the computer from malicious programs, including malware that attempts to block the operation of Kaspersky Endpoint Security or even delete it from the computer.

The stability of the security system on the computer is ensured by the self-defense and remote control defense mechanisms in Kaspersky Endpoint Security.

The *Self-Defense* mechanism prevents alteration or deletion of application files on the hard drive, memory processes, and entries in the system registry.

Remote Control Defense blocks all attempts from a remote computer to control application services.

On computers that run on 64-bit operating systems and Microsoft Windows Vista, only Kaspersky Endpoint Security Self-Defense is available for preventing the alteration and deletion of application files on the hard drive and system registry entries.

ENABLING OR DISABLING SELF-DEFENSE

The Self-Defense mechanism of Kaspersky Endpoint Security is enabled by default. You can disable Self-Defense, if necessary.

➔ *To enable or disable Self-Defense:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Advanced Settings** section.

Advanced application settings are displayed in the right part of the window.

3. Do one of the following:
 - To enable the Self-Defense mechanism, select the **Enable Self-Defense** check box.
 - To disable the Self-Defense mechanism, clear the **Enable Self-Defense** check box.
4. To save changes, click the **Save** button.

ENABLING OR DISABLING REMOTE CONTROL DEFENSE

The remote control defense mechanism is enabled by default. You can disable the remote control defense mechanism, if necessary.

➤ *To enable or disable the remote control defense mechanism:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Advanced Settings** section.

Advanced application settings are displayed in the right part of the window.
3. Do one of the following:
 - To enable the remote control defense mechanism, select the **Disable remote control of system service**.
 - To disable the remote control defense mechanism, clear the **Disable remote control of system service**.
4. To save changes, click the **Save** button.

SUPPORTING REMOTE ADMINISTRATION APPLICATIONS

You may occasionally need to use a remote administration application while external control protection is enabled.

➤ *To enable the operation of remote administration applications:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.

The anti-virus protection settings are shown in the right part of the window.
3. In the **Exclusions and trusted applications** section, click the **Settings** button.

The **Trusted zone** window opens.
4. In the **Trusted zone** window, select the **Trusted applications** tab.
5. Click the **Add** button.
6. In the context menu that opens, do one of the following:
 - To find the remote administration application in the list of applications that are installed on the computer, select the **Applications** item. The **Select application** window opens.
 - To specify the path to the executable file of the remote administration application, select **Browse**. The standard **Open file** window in Microsoft Windows opens.

These actions cause the **Exclusions for application** window to open.

7. Select the **Do not monitor application activity** check box.
8. In the **Exclusions for application** window, click **OK**.

The trusted application that you have added appears in the trusted applications list.

9. To save changes, click the **Save** button.

PERFORMANCE OF KASPERSKY ENDPOINT SECURITY AND COMPATIBILITY WITH OTHER APPLICATIONS

This section contains information about the performance of Kaspersky Endpoint Security and compatibility with other applications, in addition to guidelines for selecting the types of detectable threats and the operating mode of Kaspersky Endpoint Security.

IN THIS SECTION:

About the performance of Kaspersky Endpoint Security and compatibility with other applications	219
Selecting types of detectable threats	220
Enabling or disabling Advanced Disinfection technology	221
Enabling or disabling energy-saving mode.....	221
Enabling or disabling conceding of resources to other applications	222

ABOUT THE PERFORMANCE OF KASPERSKY ENDPOINT SECURITY AND COMPATIBILITY WITH OTHER APPLICATIONS

Performance of Kaspersky Endpoint Security

The performance of Kaspersky Endpoint Security means the number of detectable threat types, energy consumption, and use of computer resources.

Selecting types of detectable threats

Kaspersky Endpoint Security allows you to flexibly configure the protection of your computer and to select the types of threats (see the section "Selecting types of detectable threats" on page [220](#)) that the application detects. Kaspersky Endpoint Security always scans the operating system for viruses, worms, and Trojans. You cannot disable scanning of these threat types. Such malware can cause significant harm to the computer. For greater security on your computer, you can expand the range of detectable threat types by enabling monitoring of legitimate applications that an intruder can hijack to harm the computer or user data.

Using energy-saving mode

Energy consumption by applications is a key consideration for portable computers. Kaspersky Endpoint Security scheduled tasks usually use up considerable resources. When the computer is running on battery power, you can use energy-saving mode to consume power more sparingly.

In energy-saving mode, the following scheduled tasks are postponed automatically:

- Update task (see the section "About database and application module updates" on page [159](#));

- Full Scan task (see the section "About scan tasks" on page [168](#));
- Critical Areas Scan task (see the section "About scan tasks" on page [168](#));
- Custom Scan task (see the section "About scan tasks" on page [168](#));
- Vulnerability Scan task (see the section "About the Vulnerability Scan task" on page [184](#)).

Conceding computer resources to other applications

Use of computer resources by Kaspersky Endpoint Security may impact the performance of other applications. To resolve the problem of simultaneous operation with increased load on the CPU and on the hard drive subsystems, Kaspersky Endpoint Security can suspend scheduled tasks and concede resources to other applications (see the section "Enabling or disabling energy-saving mode" on page [221](#)).

However, a number of applications start immediately when CPU resources become available, proceeding to work in background mode. To prevent scanning from depending on the performance of other applications, it is better to not concede operating system resources to them.

You can start such tasks manually, if necessary.

Using advanced disinfection technology

Today's malicious programs can penetrate the lowest levels of an operating system, which makes them virtually impossible to eliminate. After detecting malicious activity in the operating system, Kaspersky Endpoint Security performs an extensive disinfection procedure that uses a special Advanced Disinfection technology (see the section "Enabling or disabling Advanced Disinfection technology" on page [221](#)). *The advanced disinfection technology* is aimed at purging the operating system of malicious programs that have already started their processes in the operating system and that prevent Kaspersky Endpoint Security from removing them by using other methods. As a result, the threat is neutralized and eliminated from the computer. While the advanced disinfection procedure is in progress, you are advised to not start new processes or edit the operating system registry. The advanced disinfection technology uses considerable operating system resources, which may slow down other applications.

After completing the advanced disinfection procedure, Kaspersky Endpoint Security restarts the system without notifying the user. We therefore recommend that you save your work and quit all applications as soon as an active infection is reported. Immediately after restarting the computer, Kaspersky Endpoint Security completes the removal of malicious program files.

After the computer restarts, we recommend that you start a Full Scan task.

SELECTING TYPES OF DETECTABLE THREATS

➔ *To select types of detectable threats:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.

The anti-virus protection settings are shown in the right part of the window.

3. In the **Threats** section, click the **Settings** button.

The **Threats** window opens.

4. Select check boxes opposite the types of threats that you want Kaspersky Endpoint Security to detect:
 - **Malicious tools**
 - **Adware**

- **Auto-dialers**
 - **Other**
 - **Packed files that may cause harm**
 - **Multi-packed files**
5. Click **OK**.

The **Threats** window closes. In the **Threats** section, the selected types of threats are listed under **Detection of the following threat types is enabled**.

6. To save changes, click the **Save** button.

ENABLING OR DISABLING ADVANCED DISINFECTION TECHNOLOGY

Advanced disinfection technology is available if Kaspersky Endpoint Security is installed on a computer that runs under Microsoft Windows for workstations. Advanced disinfection technology is unavailable if Kaspersky Endpoint Security is installed on a computer that runs under Microsoft Windows for file servers (see the section "Hardware and software requirements" on page [19](#)).

➔ *To enable or disable Advanced Disinfection technology:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Anti-Virus protection** section.
The anti-virus protection settings are shown in the right part of the window.
3. In the right part of the window, do one of the following:
 - Select the **Enable Advanced Disinfection technology** to enable advanced disinfection technology.
 - Clear the **Enable Advanced Disinfection technology** to disable advanced disinfection technology.
4. To save changes, click the **Save** button.

ENABLING OR DISABLING ENERGY-SAVING MODE

➔ *To enable or disable energy-saving mode:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Advanced Settings** section.
Advanced application settings are displayed in the right part of the window.
3. Perform the following actions in the **Operation modes** section:
 - To enable energy conservation mode, select the **Do not start scheduled tasks while running on battery power** check box.

When energy-saving mode is enabled, the following tasks are not run, even if scheduled:

- Update task
- Full Scan task

- Critical Areas Scan task
 - Custom Scan task
 - Vulnerability Scan task
- To disable energy conservation mode, clear the **Do not start scheduled tasks while running on battery power** check box.
4. To save changes, click the **Save** button.

ENABLING OR DISABLING CONCEDED OF RESOURCES TO OTHER APPLICATIONS

➤ *To enable or disable conceding of resources to other applications:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, select the **Advanced Settings** section.

Advanced application settings are displayed in the right part of the window.

3. Perform the following actions in the **Operation modes** section:

To enable the mode in which resources are conceded to other applications, select the **Concede resources to other applications** check box. When configured to concede resources to other applications, Kaspersky Endpoint Security postpones scheduled tasks that slow down other applications:

- Update task
 - Full Scan task
 - Critical Areas Scan task
 - Custom Scan task
 - Vulnerability Scan task
- To disable the mode in which resources are conceded to other applications, clear the **Concede resources to other applications** check box. In this case Kaspersky Endpoint Security carries out scheduled tasks regardless of the operation of other applications.

By default, the application is configured not to concede resources to other applications.

4. To save changes, click the **Save** button.

PASSWORD PROTECTION

This section contains information on restricting access to Kaspersky Endpoint Security with a password.

IN THIS SECTION:

About restricting access to Kaspersky Endpoint Security.....	223
Enabling and disabling password protection	223
Modifying the Kaspersky Endpoint Security access password.....	225

ABOUT RESTRICTING ACCESS TO KASPERSKY ENDPOINT SECURITY

Multiple users with different levels of computer literacy can share a single PC. If users have unrestricted access to Kaspersky Endpoint Security and its settings, the overall level of computer protection may be reduced.

You can restrict access to Kaspersky Endpoint Security by setting a password and specifying operations for which the application prompts the user for a password:

- All operations (except threat notifications)
- Editing application settings
- Quitting the application
- Disabling protection components and stopping scan tasks
- Disabling control components
- Suspending a full scan task
- Deleting the license
- Removing the application

ENABLING AND DISABLING PASSWORD PROTECTION

◆ *To enable or disable password protection:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Interface**.

The user interface settings are displayed in the right part of the window.

3. To restrict access to Kaspersky Endpoint Security with a password:
 - a. Select the **Enable password protection** check box.
 - b. Click the **Settings** button.

The **Password protection** window opens.

- c. In the **New password** field, type a password for accessing the application.

- d. Confirm the password in the **Password confirmation** field.
- e. In the **Password area** section, specify the operations with the application for which the user must enter the password:
 - To restrict access to all operations with the application, select the **All operations (except threat notifications)** setting
 - To specify individual operations, select the **Individual operations** setting.
- f. If you select the **Individual operations** setting, select the check boxes next to the names of the necessary operations:
 - **Configuring application settings.**
 - **Quitting the application.**
 - **Disabling protection components and stopping scan tasks.**
 - **Disabling control components.**
 - **Deleting the license.**
 - **Removing the application.**
- g. Click **OK**.

We recommend exercising care when you use a password to restrict access to the application. If you forget the password, contact Kaspersky Lab Technical Support for instructions on removing password protection (<http://support.kaspersky.com/helpdesk.html>).

4. To cancel password restriction of access to Kaspersky Endpoint Security:
 - a. Clear the **Enable password protection** check box.
 - b. Click the **Save** button.

The application then checks whether canceling password protection is a restricted operation.

- If the operation of canceling password protection for the application is not password protected, the restriction on access to Kaspersky Endpoint Security is removed.
 - If the operation of cancelling password protection is password-protected, the **Password verification** window appears. This window appears every time that the user performs a password-protected operation.
- c. In the **Password verification** window, type the password in the **Password** field.
 - d. If you do not want the application to prompt you for the password when you attempt this operation again during the current session, select the **Save password for current session** check box. The restriction on access to Kaspersky Endpoint Security is removed the next time that the application is started.

When the **Save password for current session** check box is cleared, the application prompts you for the password every time that you attempt this operation.
 - e. Click **OK**.

5. To save changes, in the application settings window, click the **Save** button.

MODIFYING THE KASPERSKY ENDPOINT SECURITY ACCESS PASSWORD

➔ *To change the access password for Kaspersky Endpoint Security:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Interface**.
The user interface settings are displayed in the right part of the window.
3. If password protection is disabled, select the **Enable password protection** check box.
4. Click the **Settings** button.

The **Password protection** window opens.

5. In the **Old password** field, enter the current password for accessing the application.
6. In the **New password** field, enter a new password for accessing the application.
7. In the **Password confirmation** field, enter the new password again.
8. Click **OK**.

The application verifies the values entered:

- If the old password is entered correctly, and the values of the new and confirmation passwords match, the new password is set.

The **Password protection** window closes.

- If the old password is entered incorrectly, a pop-up message appears in the **Old password** field and prompts you to try again. To do so, repeat step 5 of these instructions and click **OK**.

The **Password protection** window closes.

- If the confirmation password is entered incorrectly, a pop-up message appears in the **Password confirmation** field and prompts you to try again. To do so, repeat step 7 of these instructions and click **OK**.

The **Password protection** window closes.

9. To save changes, in the application settings window, click the **Save** button.

REMOTE ADMINISTRATION THROUGH KASPERSKY SECURITY CENTER

This section describes Kaspersky Endpoint Security administration through Kaspersky Security Center.

IN THIS SECTION:

Managing Kaspersky Endpoint Security.....	226
Managing tasks	228
Managing policies	233
Viewing user complaints in the Kaspersky Security Center event storage	235

MANAGING KASPERSKY ENDPOINT SECURITY

Kaspersky Security Center is designed for centralized processing of the primary administrative tasks involved in managing a LAN anti-virus security system that is based on applications in the Kaspersky Open Space Security product family. Kaspersky Security Center supports interaction through all network configurations that use the TCP/IP protocol.

Kaspersky Security Center makes it possible to start and stop Kaspersky Endpoint Security on a client computer and to remotely configure application settings.

IN THIS SECTION:

Starting and stopping Kaspersky Endpoint Security on a client computer	226
Configuring Kaspersky Endpoint Security settings.....	227

STARTING AND STOPPING KASPERSKY ENDPOINT SECURITY ON A CLIENT COMPUTER

➤ *To start or stop Kaspersky Endpoint Security on a client computer:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select the computer on which you want to start or stop Kaspersky Endpoint Security.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.

- In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. In the client computer properties window, select the **Applications** section.

A list of Kaspersky Lab applications that are installed on the client computer appears in the right part of the client computer properties window.


7. Select the application Kaspersky Endpoint Security 8 for Windows.
8. Do the following:

- To start Kaspersky Endpoint Security, click the  button on the right of the list of Kaspersky Lab applications or do the following:

- a. Right-click to display the context menu of Kaspersky Endpoint Security 8 for Windows and select **Properties**, or click the **Properties** button under the list of Kaspersky Lab applications.

The **Kaspersky Endpoint Security 8 for Windows application settings** window opens on the **General** tab.

- b. Click the **Start** button.

- To stop Kaspersky Endpoint Security, click the  button on the right of the list of Kaspersky Lab applications or do the following:

- a. Right-click to display the context menu of Kaspersky Endpoint Security 8 for Windows and select **Properties**, or click the **Properties** button under the list of applications.

The **Kaspersky Endpoint Security 8 for Windows application settings** window opens on the **General** tab.

- b. Click the **Stop** button.

CONFIGURING KASPERSKY ENDPOINT SECURITY SETTINGS

➔ *To configure Kaspersky Endpoint Security settings, do the following:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select the computer for which you want to configure Kaspersky Endpoint Security settings.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.
 - In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. In the client computer properties window, select the **Applications** section.

A list of Kaspersky Lab applications that are installed on the client computer appears in the right part of the client computer properties window.

7. Select the application Kaspersky Endpoint Security 8 for Windows.
8. Do one of the following:
 - Right-click to bring up the context menu of Kaspersky Endpoint Security 8 for Windows. Select **Properties**.
 - Under the list of Kaspersky Lab applications, click the **Properties** button

The **Kaspersky Endpoint Security 8 for Windows applications settings** window opens.

9. In the **Advanced Settings** section, configure Kaspersky Endpoint Security settings along with report and storage settings.

The other sections of the **Kaspersky Endpoint Security 8 for Windows application settings** window are the same as in the Kaspersky Security Center application and are described in the *Kaspersky Security Center Administrator Guide*.

If an application is subject to a policy which prohibits changes to specific settings, you cannot edit them while configuring application settings.

10. To save your changes, in the **Kaspersky Endpoint Security 8 for Windows application settings** window, click **OK**.

MANAGING TASKS

This section describes how to manage tasks for Kaspersky Endpoint Security. View the *Kaspersky Security Center Administrator Guide* for details on the concept of task management through Kaspersky Security Center.

IN THIS SECTION:

About tasks for Kaspersky Endpoint Security.....	228
Creating a local task.....	229
Creating a group task.....	230
Creating a task for a set of computers	230
Starting, stopping, suspending, and resuming a task.....	230
Editing task settings	232

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 license 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 a separate client computer

- Group tasks that are configured for client computers within one or more administration groups
- Tasks for sets of computers outside administration groups

Tasks for sets of computers outside administration groups apply only to 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 manage Kaspersky Endpoint Security remotely, you can use the following tasks:

- **Inventory.** During this task, Kaspersky Endpoint Security collects information about all application executable files that are stored on the computers.
- **Update.** During this task, Kaspersky Endpoint Security updates application databases and modules according to the configured update settings.
- **Rollback.** During this task, Kaspersky Endpoint Security rolls back the last database and module update.
- **Virus scan.** During this task, Kaspersky Endpoint Security scans the computer areas that are specified in the task settings for viruses and other threats.
- **Vulnerability Scan.** During this task, Kaspersky Endpoint Security scans installed applications for vulnerabilities.
- **Key file installation.** During this task, Kaspersky Endpoint Security installs a key file to activate the application or to install an additional license.

You can perform the following actions with tasks:

- Start, stop, suspend, and resume tasks.
- Create new tasks.
- Edit task settings.

CREATING A LOCAL TASK

➔ *To create a local task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select a computer for which you want to create a local task.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.
 - In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. Select the **Tasks** tab.
7. Click the **Add** button.

The Task Wizard starts.

8. Follow the instructions of the Task Wizard.

CREATING A GROUP TASK

➤ *To create a group task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, open the **Administered computers** folder.
3. In the results pane, select the **Tasks** tab.
4. Do one of the following:
 - Click the **Create task** button.
 - Right-click to display the context menu. Select **Create** → **Task**.

The Task Wizard starts.

5. Follow the instructions of the Task Wizard.

CREATING A TASK FOR A SET OF COMPUTERS

➤ *To create a task for a set of computers:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, open the **Tasks for sets of computers** folder.
3. Do one of the following:
 - Click the **Create task** button.
 - Right-click to display the context menu. Select **Create** → **Task**.

The Task Wizard starts.

4. Follow the instructions of the Task Wizard.

STARTING, STOPPING, SUSPENDING, AND RESUMING A TASK

If the Kaspersky Endpoint Security application is running on a client computer, you can start, stop, suspend, and resume a task on this client computer through Kaspersky Security Center. When Kaspersky Endpoint Security is suspended, running tasks are suspended and it becomes impossible to start, stop, suspend, or resume a task through Kaspersky Security Center.



➤ *To start, stop, suspend, or resume a local task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.

4. In the list of client computers, select the computer on which you want to start, stop, suspend, or resume a local task.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.
 - In the **Actions** menu, select **Computer properties**.



A client computer properties window opens.

6. Select the **Tasks** tab.
- A list of local tasks appears in the right part of the window.
7. Select a local task that you want to start, stop, suspend, or resume.
 8. Do one of the following:

- Right-click to display the context menu of the local task. Select **Start / Stop / Suspend / Resume**.
- To start or stop a local task, click the  /  button on the right of the local tasks list.
- Under the local tasks list, click the **Properties** button. The **<Task name> task properties** window opens. In the **<Task name> task properties** window, on the **General** tab, click the **Start, Stop, Suspend, or Resume** button.



➤ *To start, stop, suspend, or resume a group task:*

1. Open the Administration Console of Kaspersky Security Center.
 2. In the **Administered computers** folder of the console tree, select the folder with the name of the administration group for which you want to start, stop, suspend or resume a group task.
 3. In the results pane, select the **Tasks** tab.
- A list of group tasks appears in the right part of the window.
4. In the group tasks list select a group task that you want to start, stop, suspend, or resume.
 5. Do one of the following:
 - Right-click to display the context menu of the group task. Select **Start / Stop / Suspend / Resume**.

- Click the  /  button on the right of the group tasks list to start or stop a group task.

➤ *To start, stop, suspend, or resume a task for a set of computers:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Tasks for sets of computers** folder of the console tree, select a task for a set of computers that you want to start, stop, suspend, or resume.
3. Do one of the following:
 - Right-click to display the context menu of the task for a set of computers. Select **Start / Stop / Suspend / Resume**.

- To start or stop a task for a set of computers, click the  /  button on the right of the list of tasks for sets of computers.

EDITING TASK SETTINGS

The Kaspersky Endpoint Security task settings that you can configure through Kaspersky Security Center are identical to the task settings that you can configure through the local interface of Kaspersky Endpoint Security. You can configure the task settings when you create a task or edit its settings after the task is created.

➤ *To edit the settings of a local task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Computers** tab.
4. In the list of client computers, select the computer for which you want to configure Kaspersky Endpoint Security settings.
5. Do one of the following:
 - Right-click to display the context menu of the client computer. Select **Properties**.
 - In the **Actions** menu, select **Computer properties**.

A client computer properties window opens.

6. Select the **Tasks** section.

A list of local tasks appears in the right part of the window.
7. Select the necessary local task in the local tasks list.
8. Do one of the following:
 - Right-click to display the context menu of the task. Select **Properties**.
 - Click the **Properties** button.

The **<Local task name> properties** window opens.
9. In the **<Local task name> task properties** window, select the **Settings** section.
10. Edit the local task settings.
11. To save your changes, in the **Properties: <Local task name>** window, click **OK**.

➤ *To edit the settings of a group task:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder, open the folder with the name of the necessary administration group.
3. In the results pane, select the **Tasks** tab.

A list of group tasks appears in the lower part of the tasks pane.

4. Select the necessary group task in the group tasks list.
5. Do one of the following:
 - Right-click to display the context menu of the task. Select **Properties**.
 - On the right of the group tasks list, click the **Edit task settings** button.

The **Properties: <Group task name>** window opens.

6. In the **Properties: <Group task name>** window, select the **Settings** section.
7. Edit the group task settings.
8. To save your changes, in the **Properties: <Group task name>** window, click **OK**.

➤ *To edit the settings of a task for a set of computers:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Tasks for sets of computers** folder of the console tree, select a task for a set of computers whose settings you want to edit.
3. Do one of the following:
 - Right-click to display the context menu of the task for a set of computers. Select **Properties**.
 - On the right of the list of tasks for sets of computers, click the **Edit task settings** button

The **Properties: <Name of the task for a set of computers>** window opens.

4. In the **Properties: <Name of the task for a set of computers>** window, select the **Settings** section.
5. Edit the settings of the task for a set of computers.
6. To save your changes, in the **Properties: <Name of the task for a set of computers>** window, click **OK**.

Except for the **Settings** tab, all tabs in the task properties window are identical to those that are used in Kaspersky Security Center. Consult the *Kaspersky Security Center Administrator Guide* for their detailed description. The **Settings** tab contains settings that are specific to Kaspersky Endpoint Security. The content of the tab varies depending on the task type that is selected.

MANAGING POLICIES

This section discusses the creation and configuration of policies for Kaspersky Endpoint Security 8 for Windows. View the *Kaspersky Security Center Administrator Guide* for details on the concept of policy management through Kaspersky Security Center.

IN THIS SECTION:



About policies.....	234
Creating a policy	234
Editing policy settings.....	235

ABOUT POLICIES

You can use policies to apply identical Kaspersky Endpoint Security settings to all client computers within an administration group.

Policy-configured settings can be reconfigured for specific computers within the administration group. You can do so locally by using Kaspersky Endpoint Security. You can locally reconfigure only settings that the policy does not block from editing.

Whether an application setting on a client computer can be edited is determined by the "lock" status of the setting within a policy:

- When a setting is "locked" () , you cannot edit the setting locally, and the policy-configured setting is applied to all client computers within the administration group.
- When a setting is "unlocked" () , you can edit the setting locally. A locally configured setting is applied to all client computers within the administration group. The policy-configured setting is not applied.

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

You can perform the following operations with a policy:

- Create a policy.
- Edit policy settings.
- Delete a policy.
- Change policy status.

Consult the *Kaspersky Security Center Administrator Guide* for details on using policies that are unrelated to interaction with Kaspersky Endpoint Security.

CREATING A POLICY

➡ *To create a policy:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the administration group to which the relevant client computer belongs.
3. In the results pane, select the **Policies** tab.
4. Do one of the following:
 - Click the **Create policy** button.
 - Right-click to display the context menu. Select **Create** → **Policy**.

The Policy Wizard starts.

5. Follow the instructions of the Policy Wizard.

EDITING POLICY SETTINGS

➔ *To edit policy settings:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the **Administered computers** folder of the console tree, open the folder with the name of the relevant administration group for which you want to edit policy settings.
3. In the results pane, select the **Policies** tab.
4. Select the necessary policy.
5. Do one of the following:
 - Right-click to bring up the context menu of the policy. Select **Properties**.
 - On the right of the list of policies, click the **Edit policy** button.

The **Properties: <Policy name>** window opens.

The Kaspersky Endpoint Security 8 policy settings include the task settings (see the section "Configuring task settings" on page [232](#)) and application settings (see the section "Configuring Kaspersky Endpoint Security settings" on page [227](#)). The **Protection** and **Control** sections of the **Properties: <Policy name>** window list task settings, while the **Advanced settings** section lists application settings.

6. Edit the policy settings.
7. To save your changes, in the **Properties: <Policy name>** window, click **OK**.

VIEWING USER COMPLAINTS IN THE KASPERSKY SECURITY CENTER EVENT STORAGE

The Application Startup Control (see the section "Editing Application Startup Control message templates" on page [119](#)), Device Control (see the section "Editing templates of Device Control messages" on page [144](#)), and Web Control (see the section "Editing templates of Web Control messages" on page [157](#)) components have functionality that enables LAN users with computers that have Kaspersky Endpoint Security installed to send complaint messages.

Complaint messages can be delivered in two ways:

- As an event in the Kaspersky Security Center event storage. A user complaint is sent to the Kaspersky Security Center event storage if the copy of Kaspersky Endpoint Security that is installed on the user's computer works under an active policy.
- As an email message. A user complaint is sent as an email message if the copy of Kaspersky Endpoint Security that is installed on the user's computer does not work under a policy or works under a mobile policy.

➔ *To view a user complaint in the Kaspersky Security Center event storage:*

1. Open the Administration Console of Kaspersky Security Center.
2. In the console tree, open the folder **Event selections \ Events \ Warnings**.

The Kaspersky Security Center workspace lists all warning events, including complaints, that are received from users on the local area network. The Kaspersky Security Center workspace is located to the right of the console tree.

3. Select a complaint event in the list of events.

4. Open the event properties in one of the following ways:
 - Double-click an event in the list.
 - Right-click to display the context menu of the event In the context menu of the event, select **Properties**.
 - On the right of the list of events, click the **Open event properties** button.

PARTICIPATING 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:

About participation in Kaspersky Security Network	237
Enabling and disabling use of Kaspersky Security Network	238
Checking the connection to Kaspersky Security Network	238

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 for gathering this data.

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

Thanks to users who participate in Kaspersky Security Network, Kaspersky Lab is able to promptly gather information about types and sources of new threats, develop solutions for neutralizing them, and minimize the number of false positives.

Participation in Kaspersky Security Network also lets you access reputation statistics for applications and websites.

When you participate in Kaspersky Security Network, certain statistics are collected while Kaspersky Endpoint Security is running and are automatically sent to Kaspersky Lab.

If the computer is managed by the Administration Server of Kaspersky Security Center, the *KSN Proxy* service can be used.

KSN Proxy is a service that allows interaction between Kaspersky Security Network and the user's computer.

KSN Proxy 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 *Administrator Guide for Kaspersky Security Center*.

KSN Proxy settings can be configured in the properties of policies of *Kaspersky Security Center* (see the section "*Managing policies*" on page [233](#)).

No personal data is collected, processed, or stored. The types of data that Kaspersky Endpoint Security sends to Kaspersky Security Network are described in the KSN agreement.

Participation in Kaspersky Security Network is voluntary. The decision to participate in Kaspersky Security Network is taken during installation of Kaspersky Endpoint Security, and can be changed at any time (see the section "Enabling and disabling use of Kaspersky Security Network" on page [238](#)).

ENABLING AND DISABLING USE OF KASPERSKY SECURITY NETWORK

➤ *To enable or disable use of Kaspersky Security Network:*

1. Open the application settings window (on page [48](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **KSN Settings**.
Kaspersky Security Network settings are displayed in the right part of the window.
3. Do one of the following:
 - To enable the use of Kaspersky Security Network services, select the **Use KSN in the product** check box.
 - To disable the use of Kaspersky Security Network services, clear the **Use KSN in the product** check box.
4. To save changes, click the **Save** button.

CHECKING THE CONNECTION TO KASPERSKY SECURITY NETWORK

➤ *To check the connection to Kaspersky Security Network:*

1. Open the main application window.
2. In the upper part of the window, click the **KSN Reputation Service** button.

The **Kaspersky Security Network** window opens.

The left part of the **Kaspersky Security Network** window shows the mode of connection to Kaspersky Security Network services in the form of a round **KSN** button:

- If Kaspersky Endpoint Security is connected to Kaspersky Security Network services, the **KSN** button is green. The status that is shown under the **KSN** button reads *Enabled*. File and web resource reputation statistics are shown in the right part of the window.

Kaspersky Endpoint Security gathers statistical data on the usage of KSN when you open the **Kaspersky Security Network** window. The statistics are not updated in real time.

- If Kaspersky Endpoint Security is not connected to Kaspersky Security Network services, the **KSN** button is gray. The status that is shown under the **KSN** button reads *Disabled*.

A connection to Kaspersky Security Network may be absent for the following reasons:

- The computer is not connected to the Internet.
- You are not a participant in Kaspersky Security Network.
- Your Kaspersky Endpoint Security license is limited.

CONTACTING TECHNICAL SUPPORT

This section provides information about how to obtain technical support and the requirements for receiving help from Technical Support.

IN THIS SECTION:

How to obtain technical support	240
Collecting information for Technical Support.....	240
Technical support by phone	242
Obtaining technical support via Personal Cabinet.....	243

HOW TO OBTAIN TECHNICAL SUPPORT

If you cannot find a solution for your issue in the application documentation or in any of the sources of information about the application (see the section "Sources of information about the application" on page [13](#)), we recommend that you contact Kaspersky Lab Technical Support. Technical Support specialists will answer your questions about installing and using the application. If your computer is infected, Technical Support specialists help to fix any problems that are caused by malware.

Before contacting Technical Support, we recommend that you read through the support rules (<http://support.kaspersky.com/support/rules>).

You can contact Technical Support in one of the following ways:

- By telephone. This method allows you to consult with specialists from our Russian-language or international Technical Support.
- By sending a request from Personal Cabinet on the Technical Support website. This method allows you to contact Technical Support specialists through a request form.

To benefit from technical support, you must be a registered user of the commercial version of Kaspersky Endpoint Security 8 for Windows. Technical support is not available to users of trial versions of the application.

COLLECTING INFORMATION FOR TECHNICAL SUPPORT

After you inform Technical Support specialists about your issue, they may ask you to create a *trace file*. The trace file allows you to trace the process of performing application commands step by step and determine the stage of application operation at which an error occurs.

Technical Support specialists may also require additional information about the operating system, processes that are running on the computer, detailed reports on the operation of application components, and application crash dumps.

You can collect the necessary information with the help of Kaspersky Endpoint Security. The collected information can be uploaded to the Kaspersky Lab server or saved on the hard drive to be uploaded later at your convenience.

IN THIS SECTION:

Creating a trace file	241
Sending data files to the Technical Support server	241
Saving data files on the hard drive	242

CREATING A TRACE FILE

➤ *To create a trace file:*

1. Open the main application window (on page [46](#)).
2. In the lower part of the main application window, click the **Support** link to open the **Support** window.
3. In the **Support** window, click the **System tracing** button.

The **Technical Support Information** window opens.

4. 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)**.

5. To start the trace process, click the **Enable** button.
6. Reproduce the situation in which the problem occurred.
7. To stop the trace process, click the **Disable** button.

After a trace file is created, you can proceed to uploading tracing results to the Kaspersky Lab server (see the section "Sending data files to the Technical Support server" on page [241](#)).

SENDING DATA FILES TO THE TECHNICAL SUPPORT SERVER

You need to send the archive with information about the operating system, traces, and memory dumps to Kaspersky Lab Technical Support specialists.

You need a request number to upload data files to the Technical Support server. This number is available in your Personal Cabinet, on the Technical Support website, if your support request is active.

➤ *To send the data files to the Technical Support server:*

1. Open the main application window (on page [46](#)).
2. In the lower part of the main application window, click the **Support** link to open the **Support** window.
3. In the **Support** window, click the **System tracing** button.

The **Technical Support Information** window opens.

4. In the **Technical Support Information** window that opens, in the **Actions** section, click the **Upload support information to server** button.

The **Uploading support information to server** window opens.

5. In the **Uploading support information to server** window, select check boxes next to the files that you want to send to Technical Support.
6. Click the **Send** button.

The **Request number** window opens.

7. In the **Request number** window, specify the number that was assigned to your request when you contacted Technical Support through Personal Cabinet.
8. Click **OK**.

The selected data files are packed and sent to the Technical Support server.

SAVING DATA FILES ON THE HARD DRIVE

If you are unable to contact Technical Support for any reason, the data files can be stored on your computer and sent later from Personal Cabinet.

➔ *To save data files on the hard drive:*

1. Open the main application window (on page [46](#)).
2. In the lower part of the main application window, click the **Support** link to open the **Support** window.
3. In the **Support** window, click the **System tracing** button.

The **Technical Support Information** window opens.

4. In the **Technical Support Information** window that opens, in the **Actions** section, click the **Upload support information to server** button.

The **Uploading support information to server** window opens.

5. In the **Uploading support information to server** window, select check boxes next to the data files that you want to send to Technical Support.
6. Click the **Send** button.

The **Request number** window opens.

7. In the **Request number** window, click the **Cancel** button.
8. In the window that opens, confirm saving data files on the hard drive by clicking the **Yes** button.

A standard Microsoft Windows window for saving the archive in opens.

9. In the **File name** field, specify the name of the archive and click the **Save** button.

TECHNICAL SUPPORT BY PHONE

If an urgent issue arises, you can call specialists from Russian-speaking or international Technical Support by phone (<http://support.kaspersky.com/support/international>).

Before contacting Technical Support, please collect information (<http://support.kaspersky.com/support/details>) about your computer and the anti-virus software that is installed on it. This will allow our specialists to help you more quickly.

OBTAINING TECHNICAL SUPPORT VIA PERSONAL CABINET

Personal Cabinet is your personal area (<https://support.kaspersky.com/ru/personalcabinet?LANG=en>) on the Technical Support website.

To access Personal Cabinet, complete registration on the registration page (<https://support.kaspersky.com/ru/personalcabinet/registration/?LANG=en>) and receive a customer ID and password for accessing Personal Cabinet. To do this, you must specify an activation code (see the section "About activation code" on page 39) or a key file (see the section "About the key file" on page 40).

In Personal Cabinet, you can perform the following actions:

- Contact Technical Support and the Virus Lab.
- Contact Technical Support without using email.
- Track the status of your requests in real time.
- View a detailed history of your Technical Support requests.
- Receive a copy of the key file if it is lost or deleted.

Technical Support by email

You can send an online request to Technical Support in English, Russian, German, French, or Spanish.

Specify the following data in the fields of the online request form:

- Request type
- Application name and version number
- Request description
- Customer ID and password
- Email address

Online request to the Virus Lab

Some requests must be sent to the Virus Lab instead of Technical Support.

You can send requests of the following types to the Virus Lab:

- *Unknown malicious program* – You suspect that a file contains a virus, but Kaspersky Endpoint Security does not identify it as infected.

Virus Lab specialists analyze malicious code that is sent. If they detect a previously unknown virus, they add a corresponding description to the database, which becomes available when updating anti-virus applications.

- *False alarm* – Kaspersky Endpoint Security classifies the file as a virus, but you are sure that the file is not a virus.

Request for description of malicious program – You want to receive the description of a virus that Kaspersky Endpoint Security detects, based on the name of the virus.

You can also send requests to the Virus Lab from the request form page (<http://support.kaspersky.com/virlab/helpdesk.html>) without being registered in Personal Cabinet. You do not have to specify the application activation code.

GLOSSARY

A

ADMINISTRATION GROUP

A set of computers that share common functions and a set of Kaspersky Lab applications that is installed on them. Computers are grouped so that they can be managed conveniently as a single unit. A group may include other groups. It is possible to create group policies and group tasks for each installed application in the group.

ADMINISTRATION KIT CONNECTOR

Application functionality that connects the application with Administration Kit. Administration Kit enables remote administration of the application through Kaspersky Security Center.

ADMINISTRATION SERVER

A component of Kaspersky Security Center that centrally stores information about all Kaspersky Lab applications that are installed within the corporate network. It can also be used to manage these applications.

APPLICATION MODULES

Files that are included in the application setup file, which implement the core functionality of the application. A separate executable module corresponds to each type of task that is performed by the application (Real-time protection, On-demand scan, Update). When starting a full scan of the computer from the main application window, you initiate the module of this task.

APPLICATION SETTINGS

Application settings that are common to all types of tasks and govern the overall operation of the application, such as application performance settings, report settings, and backup settings.

ARCHIVE

A file that "contains" one or more files which may also be archives.

AUTORUN OBJECTS

A set of applications needed for the operating system and software that is installed on the computer to start and operate correctly. The operating system launches these objects at every startup. Viruses can target precisely these objects, thus preventing the operating system from starting, for example.

B

BACKUP

A special storage for backup copies of files that are created before the first attempt at disinfection or deletion.

BLACK LIST OF ADDRESSES

A list of email addresses from which all incoming messages are blocked by the Kaspersky Lab application, regardless of the message content.

D

DATABASE OF PHISHING WEB ADDRESSES

A list of web addresses which Kaspersky Lab specialists have determined to be phishing-related. The database is regularly updated and is part of the Kaspersky Lab application distribution kit.

DATABASE OF SUSPICIOUS WEB ADDRESSES

A list of web addresses whose content may be considered to be dangerous. The list is created by Kaspersky Lab specialists. It is regularly updated and is included in the Kaspersky Lab application distribution kit.

DATABASES

Databases that are maintained by Kaspersky Lab specialists and contain detailed descriptions of all computer security threats that are currently known to Kaspersky Lab, with ways to detect and neutralize them. These databases are constantly updated by Kaspersky Lab as new threats appear.

DISINFECTION

A method of handling infected files that results in full or partial recovery of data, or a verdict that files cannot be disinfected. Files are disinfected on the basis of database records. Some data may be lost during disinfection.

F

FALSE ALARM

A false alarm occurs when the Kaspersky Lab application reports an uninfected file as infected because the signature of the file is similar to that of a virus.

FILE MASK

Representation of a file name and extension by using wildcards.

File masks can contain any characters that are allowed in file names, including wildcards:

* – Replaces any zero or more characters.

? – Replaces any one character.

Note that the file name and extension are always separated by a period.

H

HEURISTIC ANALYSIS

The technology was developed for detecting threats that cannot be detected by using the Kaspersky Lab application databases. It allows detecting files that are suspected of being infected with an unknown virus or a new modification of a known virus.

Files in which malicious code is detected during heuristic analysis are marked as potentially infected.

HEURISTIC ANALYZER

Functions in Kaspersky Endpoint Security that perform heuristic analysis.

I

INFECTABLE FILE

A file which, due to its structure or format, can be used by intruders as a "container" to store and spread malicious code. As a rule, these are executable files, with such file extensions as .com, .exe, and .dll. There is a fairly high risk of intrusion of malicious code in such files.

INFECTED FILE

A file which contains malicious code (code of a known threat has been detected when scanning the file). Kaspersky Lab does not recommend using such files, because they may infect your computer.

N**NETWORK AGENT**

A Kaspersky Security Center component that enables interaction between the Administration Server and Kaspersky Lab applications that are installed on a specific network node (workstation or server). This component is common to all Windows applications of Kaspersky Lab. Separate Network Agent versions exist for Novell, Unix, and Mac applications from Kaspersky Lab.

NORMALIZED FORM OF THE ADDRESS OF A WEB RESOURCE

The normalized form of the address of a web resource is a textual representation of a web resource address that is obtained through normalization. Normalization is a process whereby the textual representation of a web resource address changes according to specific rules (for example, exclusion of the HTTP login, password, and connection port from the text representation of the web resource address; additionally, the web resource address is changed from uppercase to lowercase characters).

In the context of anti-virus protection, the purpose of normalization of web resource addresses is to avoid scanning website addresses, which may differ in syntax while being physically equivalent, more than once.

Example:

Non-normalized form of an address: www.Example.com\.

Normalized form of an address: www.example.com.

O**OLE OBJECT**

An attached file or a file that is embedded in another file. Kaspersky Lab applications allow scanning OLE objects for viruses. For example, if you insert a Microsoft Office Excel® table into a Microsoft Office Word document, the table is scanned as an OLE object.

P**PHISHING**

A kind of Internet fraud, when email messages are sent with the purpose of stealing confidential information. As a rule, this information relates to financial data.

POTENTIALLY INFECTED FILE

A file which contains either modified code of a known virus or code that resembles that of a virus, but is not yet known to Kaspersky Lab. Potentially infected files are detected by Heuristic Analyzer.

Q**QUARANTINE**

A certain folder that stores all potentially infected files that are detected during scanning or real-time protection.

QUARANTINING OF FILES

A method of handling a potentially infected file whereby access to the file is blocked and the file is moved from its original location to the quarantine folder, where it is kept in encrypted form to rule out the threat of infection.

S

SIGNATURE ANALYSIS

A threat detection technology which uses the Kaspersky Endpoint Security database that contains descriptions of known threats and methods for eradicating them. Protection that uses signature analysis provides a minimally acceptable level of security. Following the recommendations of Kaspersky Lab's experts, this method is always enabled.

T

TASK

The functions of the Kaspersky Lab application are implemented in the form of tasks, such as: Real-time protection, Full scan, and Database update.

TASK SETTINGS

Application settings specific to each type of tasks.

U

UPDATE

The procedure of replacing or adding new files (databases or application modules) that are retrieved from Kaspersky Lab update servers.

KASPERSKY LAB ZAO

Kaspersky Lab software is internationally renowned for its protection against viruses, malware, spam, network and hacker attacks, and other threats.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred developer of computer protection systems among home users in Russia, according to the COMCON survey "TGI-Russia 2009".

Kaspersky Lab was founded in Russia in 1997. Today, it is an international group of companies headquartered in Moscow with five regional divisions that manage the company's activity in Russia, Western and Eastern Europe, the Middle East, Africa, North and South America, Japan, China, and other countries in the Asia-Pacific region. The company employs more than 2000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems—from home computers to large corporate networks.

The personal product range includes anti-virus applications for desktop, laptop, and pocket computers, and for smartphones and other mobile devices.

Kaspersky Lab delivers applications and services to protect workstations, file and web servers, mail gateways, and firewalls. Used in conjunction with Kaspersky Lab's centralized management system, these solutions ensure effective automated protection for companies and organizations against computer threats. Kaspersky Lab's products are certified by the major test laboratories, are compatible with the software of many suppliers of computer applications, and are optimized to run on many hardware platforms.

Kaspersky Lab's virus analysts work around the clock. Every day they uncover hundreds of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications. *Kaspersky Lab's Anti-Virus database is updated hourly; and the Anti-Spam database every five minutes.*

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the Kaspersky Anti-Virus kernel in their products, including: SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (UK), CommuniGate Systems (USA), Critical Path (Ireland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANdesk (USA), Microsoft (USA), NETASQ (France), NETGEAR (USA), Parallels (Russia), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Many of the company's innovative technologies are patented.

Achievements. Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. For example, in 2010 Kaspersky Anti-Virus received several top Advanced+ awards in a test administered by AV-Comparatives, a respected Austrian anti-virus laboratory. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 300 million users, and its corporate clients number more than 200,000.

Kaspersky Lab's website:

<http://www.kaspersky.com>

Virus encyclopedia:

<http://www.securelist.com>

Anti-virus laboratory:

newvirus@kaspersky.com

(only for sending probably infected files in archive format)

<http://support.kaspersky.com/virlab/helpdesk.html>

(for queries addressed to virus analysts)

Kaspersky Lab's web forum:

<http://forum.kaspersky.com>

INFORMATION ABOUT THIRD-PARTY CODE

Information about third-party code is contained in the file legal_notices.txt, in the application installation folder.

TRADEMARK NOTICES

Registered trademarks and service marks are the property of their respective owners.

Microsoft, Windows, Active Directory, Internet Explorer, Excel, Outlook, Outlook Express, Windows Vista, Windows Server are trademarks of Microsoft Corporation registered in the United States of America and elsewhere.

Intel, Pentium are the trademarks of Intel Corporation registered in the United States and elsewhere.

Adobe and Acrobat are the trademarks or registered trademarks of Adobe Systems Incorporated in the USA and / or elsewhere.

Radmin and Remote Administrator are the registered trademarks of Famatech.

Mozilla and Thunderbird are the trademarks of Mozilla Foundation.

ICQ is a trademark and / or service mark of ICQ LLC.

Mail.ru is a registered trademark of Mail.Ru LLC.

INDEX

A

Access rules	
devices	139
web resources	150
Activating the application.....	31
by using activation code	32
by using the key file	32
Administration groups.....	245
Administration Server.....	245
Application group network rules	91
APPLICATION INTERFACE	45
Application network rules	98
Application Privilege Control	125
Application Control rules.....	129
Application Self-Defense	217
Application Startup Control.....	111
Application Startup Control rules	113
operating modes.....	120

B

Backup	202, 208
configuring settings.....	203
deleting an object	209
restoring an object	208

C

Control rules	
application startup	113
applications.....	129

D

Database of phishing web addresses	
IM Anti-Virus	82
Web Anti-Virus.....	76
Databases	159
Device Control.....	137
device access rules	139

E

End User License Agreement	23, 38
----------------------------------	--------

F

File Anti-Virus	
enabling and disabling	51
heuristic analysis	56
protection scope	55
scan optimization.....	58
scanning of compound files	58
security level.....	54
File Anti-Virus.....	57
Firewall.....	84

H

Hardware requirements.....	19
Heuristic analysis	
File Anti-Virus	56
IM Anti-Virus	83
Mail Anti-Virus	70
Web Anti-Virus.....	77

I

IM Anti-Virus	
database of phishing web addresses	82
enabling and disabling	80
heuristic analysis	83
protection scope	82
Installing the application	21

K

KASPERSKY LAB ZAO	249
Key file	40

L

License.....	39
activating the application	41
End User License Agreement.....	38
information.....	42
key file	40
managing.....	41
renewing.....	42

M

Mail Anti-Virus	
enabling and disabling.....	64
heuristic analysis	70
protection scope	67
scanning	69
security level.....	67
Main application window	46
Monitoring network traffic	106

N

Network Attack Blocker	104
Network connection status	86
Network Monitor	110
Network packet rules.....	87
Network rules	85
Notifications.....	199
configuring settings.....	199

P

Protection scope	
File Anti-Virus	55
IM Anti-Virus	82
Mail Anti-Virus	67

Q

Quarantine	204
configuring settings.....	203
deleting an object	207

restoring an object	206
R	
Remote administration	
policies.....	233
tasks	228
Remote administration of the application	226
Removing the application	35
Reports	
configuring settings.....	194
generating.....	195
Restricting access to the application	223
password protection	223
Run task	
scanning	169
update.....	165
Vulnerability Scan.....	184
S	
Scan scope	172
Scanning	
action to take on a detected object	171
run mode	175
running a task	169, 175
scan optimization.....	173
scan scope	172
scan technologies.....	175
scanning of compound files	174
scanning of removable drives	177
security level.....	171
tasks	168
Settings	
initial configuration.....	30
Software requirements	19
START	
APPLICATION.....	49
System Watcher.....	61
T	
Trusted applications	215
Trusted devices.....	139
Trusted zone	210
exclusion rule.....	212
settings	212
trusted applications.....	215, 216
U	
Update.....	159
application modules	159
application version.....	33
proxy server	166
rolling back the last update	166
update source.....	160, 161
Update source.....	160
V	
Vulnerability.....	188
Vulnerability Monitor.....	182
Vulnerability Scan task.....	184

run mode	185
starting and stopping	184

W

Web Anti-Virus	
database of phishing web addresses	76
enabling and disabling	73
heuristic analysis	77
security level.....	75
Web Control	148