



Kaspersky Security for Virtualization 4.0 Light Agent for Windows

User Guide for Windows

Application version: 4.0

Dear User,

Thank you for your trust. 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 AO Kaspersky Lab (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.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any third-party materials used herein, or for any potential harm associated with the use of such materials.

Document revision date: 20/1/2017

© 2017 AO Kaspersky Lab. All Rights Reserved.

<http://www.kaspersky.com>

<https://help.kaspersky.com>

<http://support.kaspersky.com>

Contents

About this Guide	11
In this document	11
Document conventions	15
Kaspersky Security for Virtualization 4.0 Light Agent	17
Application interface	21
Application icon in the taskbar notification area	21
Enabling and disabling the animation of the application icon.....	22
Application icon context menu	23
Main application window	23
Application settings window	25
Starting and stopping the application	26
Enabling and disabling automatic startup of the application	26
Starting and stopping the application manually	27
Pausing and resuming virtual machine protection and control.....	27
Virtual machine protection state.....	29
Virtual machine protection status indication.....	29
Resolving virtual machine protection problems	31
Connection of a protected virtual machine to an SVM	32
Connecting a protected virtual machine to an SVM.....	32
Configuring SVM discovery settings	33
Protecting the file system of a virtual machine. File Anti-Virus.....	36
A bout File Anti-Virus	36
Enabling and disabling File Anti-Virus	37
Configuring File Anti-Virus	38
Automatically pausing File Anti-Virus	40
Changing the file security level.....	41
Changing the File Anti-Virus action to take on infected files.....	42
Editing the protection scope of File Anti-Virus	43
Configuring the usage of Heuristic Analyzer with File Anti-Virus	45
Configuring the usage of iSwift technology in the operation of File Anti-Virus.....	46

Optimizing file scanning by File Anti-Virus.....	47
Scanning of compound files by File Anti-Virus	47
Changing the scan mode.....	49
Email protection. Mail Anti-Virus	50
About Mail Anti-Virus	50
Enabling and disabling Mail Anti-Virus.....	51
Configuring Mail Anti-Virus	53
Changing the mail security level.....	54
Changing the action to take on infected email messages	55
Editing the protection scope of Mail Anti-Virus	56
Filtering attachments in messages	59
Using Heuristic Analyzer with Mail Anti-Virus	60
Scanning emails in Microsoft Office Outlook	60
Protecting virtual machine web traffic. Web Anti-Virus	62
About Web Anti-Virus	62
Enabling and disabling Web Anti-Virus.....	63
Configuring Web Anti-Virus	65
Changing the web traffic security level	66
Changing the action to take on malicious web traffic objects	67
Web Anti-Virus scanning to check links against databases of phishing and malicious web addresses	67
Using Heuristic Analyzer with Web Anti-Virus	69
Configuring the duration of caching web traffic.....	69
Editing the list of trusted web addresses	71
Protection of IM client traffic. IM Anti-Virus	72
About IM Anti-Virus.....	72
Enabling and disabling IM Anti-Virus	73
Configuring IM Anti-Virus.....	75
Creating the protection scope of IM Anti-Virus	75
Scanning links against databases of malicious and phishing web addresses with IM Anti-Virus	76
Using Heuristic Analyzer with IM Anti-Virus.....	77
Network protection	78
Firewall	78

About Firewall.....	79
Enabling or disabling Firewall.....	80
About network rules.....	82
About the network connection status.....	83
Changing the network connection status.....	84
Managing network packet rules.....	84
Creating and editing a network packet rule.....	85
Enabling or disabling a network packet rule.....	89
Changing the Firewall action for a network packet rule.....	90
Changing the priority of a network packet rule.....	90
Managing network rules for application groups.....	91
Creating and editing an application group network rule.....	93
Enabling or disabling an application group network rule.....	97
Changing the Firewall action for an application group network rule.....	98
Changing the priority of an application group network rule.....	99
Managing network rules for applications.....	100
Creating and editing an application network rule.....	102
Enabling or disabling an application network rule.....	105
Changing the Firewall action for an application network rule.....	106
Changing the priority of an application network rule.....	108
Network Attack Blocker.....	109
About Network Attack Blocker.....	110
Enabling and disabling Network Attack Blocker.....	110
Editing the settings used in blocking an attacking computer.....	112
Monitoring network traffic.....	112
About network traffic monitoring.....	113
Configuring the settings of network traffic monitoring.....	113
Enabling monitoring of all network ports.....	114
Creating a list of monitored network ports.....	114
Creating a list of applications for which all network ports are monitored.....	116
Network Monitor.....	117
About Network Monitor.....	117
Starting Network Monitor.....	118

System Watcher	119
About System Watcher	119
Enabling and disabling System Watcher	120
Using behavior stream signatures (BSS).....	122
Rolling back malware actions during disinfection	122
Application Startup Control	124
About Application Startup Control.....	124
Enabling and disabling Application Startup Control	125
About Application Startup Control rules	127
About Application Startup Control operation modes	129
Managing Application Startup Control rules.....	130
Adding and editing an Application Startup Control rule	131
Adding a trigger condition for an Application Startup Control rule	132
Editing the status of an Application Startup Control rule	136
Editing Application Startup Control message templates	137
Application Privilege Control	138
About Application Privilege Control	138
Enabling and disabling Application Privilege Control	139
Placing applications into groups	141
Moving an application to a trusted group	143
Working with application control rules	144
Editing control rules for trust groups and application groups.....	144
Editing an application control rule.....	146
Disabling downloads and updates of application control rules from the Kaspersky Security Network database	147
Disabling the inheritance of restrictions from the parent process	148
Excluding specific application actions from application control rules.....	150
Configuring storage settings for control rules that govern unused applications...	151
Protecting operating system resources and personal data	151
Adding a category of protected resources	152
Adding a protected resource	153
Disabling resource protection	154
Device Control	156
About Device Control.....	157

Enabling and disabling Device Control	157
About rules of access to devices and connection buses	159
About trusted devices	159
Standard decisions on access to devices	160
Editing a device access rule	162
Editing a connection bus access rule	163
Actions with trusted devices	164
Adding a device to the list of trusted devices.....	164
Editing the Users setting of a trusted device	166
Removing a device from the list of trusted devices	166
Editing templates of Device Control messages	167
Obtaining access to a blocked device	168
Web Control.....	171
About Web Control	171
Enabling and disabling Web Control.....	172
About web resource access rules.....	174
Actions with web resource access rules	175
Adding and editing a web resource access rule	176
Rules for creating masks for web resource addresses.....	179
Exporting and importing the list of web resource addresses	182
Testing web resource access rules	184
Changing the priority web resource access rules	185
Enabling and disabling a web resource access rule.....	186
About Web Control messages	187
Editing templates of Web Control messages	187
Scanning the virtual machine.....	189
About scan tasks	189
Starting or stopping a scan task	190
Configuring scan task settings.....	191
Changing the security level	193
Changing the action to take on infected files.....	194
Editing the scan scope	195
Optimizing file scanning	199
Scanning compound files	200

Configuring Heuristic Analyzer	201
Configuring the usage of iSwift technology.....	202
Selecting the scan task run mode	203
Starting a scan task under the account of a different user.....	205
Scanning removable drives when they are connected to the virtual machine	206
Handling unprocessed files.....	207
About unprocessed files	207
Managing the list of unprocessed files	208
Starting a Custom Scan task for unprocessed files.....	209
Restoring files from the list of unprocessed files	210
Deleting files from the list of unprocessed files	211
Updating databases and application modules	212
About database and application module updates	212
Starting and stopping an update task	213
Selecting the update task run mode	214
Trusted zone.....	217
About the trusted zone.....	217
Configuring the trusted zone.....	219
Creating an exclusion	221
Editing an exclusion	223
Removing an exclusion	223
Enabling or disabling an exclusion	224
Editing the list of trusted applications	225
Including or excluding a trusted application from scanning	227
Backup.....	228
About Backup	228
Configuring backup settings	229
Configuring the maximum storage term for files in Backup	229
Configuring the maximum size of Backup	230
Managing Backup.....	231
Restoring files from Backup.....	232
Deleting backup copies of files from Backup	233

Managing Reports	234
Principles of managing reports	234
Configuring report settings.....	236
Configuring the maximum report storage term	236
Configuring the maximum size of the report file	237
Generating reports.....	238
Viewing reported event information in a separate section	238
Saving a report to file.....	239
Removing information from reports	241
Notifications	243
About Kaspersky Security notifications.....	243
Configuring notifications	244
Configuring event logging.....	244
Configuring the display of on-screen notifications	245
Configuring event notifications via email	246
Performance of Kaspersky Security.....	247
About Kaspersky Security performance	247
Selecting types of detectable objects	249
Enabling or disabling Advanced Disinfection technology for desktop operating systems	250
Kaspersky Security Self-Defense	251
About Kaspersky Security Self-Defense	251
Enabling or disabling Self-Defense.....	251
Enabling or disabling Remote Control Defense	252
Supporting remote administration applications.....	253
Password protection	254
About restricting access to the application.....	254
Enabling and disabling password protection.....	255
Managing Kaspersky Security settings	258
Importing Kaspersky Security settings into an application installed on another virtual machine	258
Restoring the default application settings	260

Participating in Kaspersky Security Network.....	262
About participation in Kaspersky Security Network	262
Checking the connection to Kaspersky Security Network.....	263
Glossary.....	265
AO Kaspersky Lab.....	269
Information about third-party code	271
Trademark notices	272
Index.....	273

About this Guide

The User Guide for Kaspersky Security for Virtualization 4.0 Light Agent (hereinafter referred to as "Kaspersky Security") is intended for specialists who configure Light Agent installed on a virtual machine running a Microsoft® Windows® operating system (hereinafter referred to as "Light agent for Windows").

To be able to use Kaspersky Security successfully, you should be acquainted with the interface of the Microsoft Windows operating system that you use, know the basic techniques of using that system, and know how to use email and the Internet.

In this section:

In this document.....	11
Document conventions.....	15

In this document

This document comprises the following sections:

Kaspersky Security for Virtualization 4.0 Light Agent (see page [17](#))

This section describes the purpose, key features, and structure of the application, as well as a brief description of application components and functions.

Application interface (see page [21](#))

This section describes the primary elements of the application interface.

Starting and stopping the application (see page [26](#))

This section describes how to start and shut down the application.

Virtual machine protection status (see page [29](#))

This section describes ways to detect security threats and configure protection against them.

Connecting a protected virtual machine to an SVM (see page [32](#))

This section provides information on the specifics of connecting a protected virtual machine to an SVM and how to configure the connection.

Protecting the file system of a virtual machine. File Anti-Virus (see page [36](#))

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

Email protection. Mail Anti-Virus (see page [50](#))

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

Protecting virtual machine web traffic. Web Anti-Virus (see page [62](#))

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

Protection of IM client traffic. IM Anti-Virus (see page [72](#))

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

Network protection (see page [78](#))

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

System Watcher (see page [119](#))

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

Application Startup Control (see page [124](#))

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

Application Privilege Control (see page [138](#))

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

Device Control (see page [156](#))

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

Web Control (see page [171](#))

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

Scanning a virtual machine (see page [189](#))

This section describes the specifics and settings of scan tasks, security levels, scan methods and technologies, and instructions on handling files that Kaspersky Security has not processed when scanning the virtual machine for viruses and other malware.

Updating databases and application modules (see page [212](#))

This section contains information about database and application module updates (also called "updates"), and instructions on how to configure update settings.

Trusted zone (see page [217](#))

This section contains information on the trusted zone and instructions on configuring exclusions and creating a list of trusted applications.

Backup (see page [228](#))

This section describes how you can configure and manage Backup.

Managing reports (see page [234](#))

This section describes how you can configure report settings and manage reports.

Notifications (see p. [243](#))

This section describes notifications alerting the user to events in the operation of Kaspersky Security and provides instructions on configuring event notifications.

Performance of Kaspersky Security and compatibility with other applications (see page [247](#))

This section contains information about the performance of Kaspersky Security and compatibility with other applications, and also guidelines for selecting the types of detectable objects and the operating mode of Kaspersky Security.

Kaspersky Security Self-Defense (see page [251](#))

This section describes the self-defense and remote control defense mechanisms of Kaspersky Security and provides instructions on configuring the settings of these mechanisms.

Password protection (see page [254](#))

This section contains information on how to restrict access to Kaspersky Security using a password.

Managing Kaspersky Security settings (see page [258](#))

This section contains instructions on transferring configured application settings to Kaspersky Security installed on a different virtual machine and restoring the standard application settings.

Participating in Kaspersky Security Network (see page [262](#))

This section covers participation in Kaspersky Security Network and provides instructions on how to check the connection to Kaspersky Security Network.

Glossary (see page [265](#))

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

AO Kaspersky Lab (see page [269](#))

This section provides information about AO Kaspersky Lab.

Information about third-party code (see page [271](#))

This section provides information about third-party code used in the application.

Trademark notices (see page [272](#))

This section lists third-party trademarks used in this document.

Index

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

Document conventions

This document uses the following conventions (see table below).

Table 1. Document conventions

Sample text	Description of document convention
Note that...	Warnings are highlighted in red and surrounded by a box. Warnings show information about actions that may have unwanted consequences.
We recommended that you use...	Notes are surrounded by a box. Notes provide additional and reference information.
Example: ...	Examples are given on a blue background under the heading "Example".
<i>Update means...</i> The <i>Databases are out of date</i> event occurs.	The following elements are italicized in the text: <ul style="list-style-type: none">• New terms• Names of application statuses and events
Press ENTER . Press ALT+F4 .	The 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. The keys must be pressed simultaneously.

Sample text	Description of document convention
Click the Enable button.	Names of application interface elements, such as text boxes, menu items, and buttons, are set off in bold.
▶ <i>To configure a task schedule:</i>	Introductory phrases of instructions are italicized and are accompanied by the arrow sign.
<p>In the command line, type <code>help</code>.</p> <p>The following message then appears:</p> <p><code>Specify the date in MM:DD:YY format.</code></p>	<p>The following types of text content are set off with a special font:</p> <ul style="list-style-type: none"> • text in the command line; • text of messages that the application displays on screen; • data that must be entered using the keyboard.
<User name>	Variables are enclosed in angle brackets. Instead of the variable, insert the corresponding value, not including the angle brackets.

Kaspersky Security for Virtualization 4.0 Light Agent

Kaspersky Security for Virtualization 4.0 Light Agent is an integrated solution providing comprehensive protection for virtual machine powered by a Microsoft® Windows Server® hypervisors in the Hyper-V® role (hereinafter also "Microsoft Windows Server (Hyper-V)"), Citrix® XenServer, VMware ESXi™ or KVM (Kernel-based Virtual Machine) hypervisor against various information threats, network and phishing attacks.

Kaspersky Security is optimized to support maximum performance of the virtual machines that you want to protect.

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

In addition to real-time protection provided by the application components, you can regularly scan the virtual machines for viruses and other threats. This helps to rule out the spread of malware that remains undetected by the application for various reasons, such as a low security level setting.

Application components

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 logs the activity of applications in the operating system that is installed on the protected virtual machine, and regulates application activity depending on the trust group the component assigns them to. A set of rules is specified for each group of applications. These rules regulate the access of applications to personal data and to operating system resources. Such personal data of the user includes the My Documents folder, cookies, information about user activity in the operating system, and files, folders, and registry keys that contain operation settings and important data of the most frequently used applications.

- **Device Control.** This component lets you set flexible restrictions on access to data storage devices (such as hard drives, removable drives, CDs and DVDs), network devices (such as modems), printing devices (such as printers), or interfaces for connecting devices to the protected virtual machine (such as USB, Bluetooth, and FireWire).
- **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.
- Application Privilege Control uses Application Control rules.
- Device Control uses device access rules and connection bus access rules.
- Web Control uses web resource access rules.

The following application components are protection components:

- **File Anti-Virus.** This component prevents infection of the file system of the protected virtual machine's operating system. File Anti-Virus starts together with Kaspersky Security, continuously remains active in computer memory, and scans all files that are opened, saved, or started in the operating system of the protected virtual machine. File Anti-Virus intercepts every attempt to access a file and scans the file for viruses and other malware.
- **System Watcher.** This component collects information about application activity in the operating system of the protected virtual machine and provides this information to other components for more effective protection.
- **Mail Anti-Virus.** This component scans incoming and outgoing email messages for viruses and other malware.
- **Web Anti-Virus.** This component scans inbound HTTP and FTP traffic of the protected virtual machine and checks links against lists of malicious and phishing web addresses.
- **IM Anti-Virus.** This component scans inbound and outbound traffic of the protected virtual machine transmitted via protocols of IM clients. The component lets you use many IM clients safely.

- **Firewall.** This component protects personal data that is stored in the operating system of the protected virtual machine and blocks all kinds of threats to the operating system while the protected virtual machine is connected to the Internet or to a local area network. The component filters all network activity in accordance with two types of rules: application network rules and network packet rules (see section "About network rules" on page [82](#)).
- **Network Monitor.** This component lets you view the network activity of the protected virtual machine 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 the protected virtual machine, Kaspersky Security blocks network activity originating from the attacking computer.

Application tasks and functions

Kaspersky Security supports the following tasks:

- **Full Scan.** Kaspersky Security thoroughly scans the operating system of the protected virtual machine, including RAM, objects that are loaded at startup, backup storage of the operating system, and all hard drives and removable drives.
- **Custom Scan.** Kaspersky Security scans objects selected by the user.
- **Critical Areas Scan.** Kaspersky Security scans objects that are loaded at startup of the protected virtual machine's operating system, RAM, and objects that are targeted by rootkits.
- **Update.** Kaspersky Security downloads updated databases and application modules. Updates keep the operating system of the protected virtual machine secure against new viruses and other malware.

Kaspersky Security includes a number of service functions designed 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 Security events and all operations that the application performs. In case of an incident, you can send reports to Kaspersky Lab, where Technical Support will look into the issue in more detail.
- **Data storage.** If the application detects infected files while scanning the protected virtual machine's operating system for viruses and other malicious programs, Kaspersky Security blocks such files. Kaspersky Security stores copies of disinfected and deleted files in *Backup*. Kaspersky Security moves files that have not been processed for any reason to the list of unprocessed files. You can restore files to their original folders and empty the data storage.
- **Notifications.** Notifications keep the user informed about the current protection status of the protected virtual machine's operating system and the operation of Kaspersky Security. Notifications can be displayed on the screen or delivered via email.
- **Support.** All registered users of Kaspersky Security can contact Technical Support for assistance. You can send a request via your Kaspersky CompanyAccount on the Technical Support website or receive help over the phone (for details, see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

Application interface

This section describes the primary elements of the application interface.

In this section:

Application icon in the taskbar notification area	21
Enabling and disabling the animation of the application icon	22
Application icon context menu	23
Main application window	23
Application settings window	25




Application icon in the taskbar notification area

As soon as Kaspersky Security starts, 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.

The application icon reflects the status of virtual machine 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 Security is scanning an email message.
- The  icon signifies that Kaspersky Security is scanning inbound and outbound network traffic.

- The 🔄 icon signifies that Kaspersky Security is updating databases and application modules.
- The ⚠️ icon signifies that important events that require your attention have occurred in the operation of Kaspersky Security. For example, File Anti-Virus is disabled or the databases and application modules are out of date.
- The 🚨 icon signifies that critical events have occurred in the operation of Kaspersky Security. For example, a failure in the operation of one or more components, or corruption of the application databases or modules.

The animation of the application icon is disabled by default. You can enable the animation of the application icon (see section "Enabling and disabling the animation of the application icon" on page [22](#)).

Enabling and disabling the animation of the application icon

► *To enable or disable the animation of an application icon:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **Interface**.

Application interface settings appear in the right part of the window.

3. Do one of the following:
 - Select the **Use icon animation while running tasks** check box to enable the animation of the application icon.
 - Clear the **Use icon animation while running tasks** check box to disable the animation of the application icon.
4. To save changes, click the **Save** button.

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.

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

- **Kaspersky Security for Virtualization 4.0 Light Agent.** 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 and scan tasks, being only available when the Kaspersky Security Center policy is disabled.
- **Disable policy / Enable policy.** Disables / enables the Kaspersky Security Center policy.
This item is unavailable when Kaspersky Security operates under a Kaspersky Security Center policy, and a password for disabling the policy has been set in the policy settings.
- **About.** This item opens an information window with application details.
- **Exit.** This item quits Kaspersky Security. Clicking this context menu item causes the application to be unloaded from the virtual machine RAM.

Main application window

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

► *To open the main window of Kaspersky Security:*

- rest the mouse pointer over the application icon in the taskbar notification area of Microsoft Windows and left-click;
- select **Kaspersky Security for Virtualization 4.0 Light Agent** in the application icon context menu (see section "Application icon context menu" on page [23](#));
- in the **Start** menu, select **Applications** → **Kaspersky Security for Virtualization 4.0 Light Agent**.

The main application window can be divided into three parts:

- 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
 - Storage of backup copies of infected files that the application has deleted or modified
 - 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** and **Settings** tabs are located in the center of the window:
 - The **Protection and Control** tab lets you manage the operation of application components and tasks. The **Protection and Control** tab is displayed when you open the main application window.
 - The **Settings** tab lets you edit the default application settings.
- The following links are located in the lower part of the window:
 - **Help**. Clicking this link takes you to the help system of Kaspersky Security.
 - **Support**. Clicking this link opens the **Support** window, which contains information on the operating system, the current version of Kaspersky Security, and links to Kaspersky Lab information resources.
 - **License**. Clicking this link opens the **Licensing** window with the details of the current license.

Application settings window

The Kaspersky Security settings window lets you configure general application settings, individual components, reports and storages, scan tasks, and update tasks.

► *To open the application settings window:*

- select the **Settings** tab in the main application window (see section "Main application window" on page [23](#)).
- select **Settings** in the application icon context menu (see section "Application icon context menu" on page [23](#)).

The application settings window consists of two parts:

- 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.

Starting and stopping the application

This section describes how to start and shut down the application.

In this section:

Enabling and disabling automatic startup of the application	26
Starting and stopping the application manually	27
Pausing and resuming virtual machine protection and control	27

Enabling and disabling automatic startup of the application

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

After installation, Kaspersky 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 (see page [25](#)).

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 **Launch Kaspersky Security for Virtualization 4.0 Light Agent when the virtual machine is turned on** check box.
- To disable automatic application startup, clear the **Launch Kaspersky Security for Virtualization 4.0 Light Agent when the virtual machine is turned on** check box.

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

Starting and stopping the application manually

Kaspersky Lab specialists do not recommend stopping Kaspersky Security manually, because doing so exposes the virtual machine and your personal data to threats. If necessary, you can pause virtual machine protection (see section "Pausing and resuming virtual machine protection and control" on page [27](#)) for as long as you need to, without stopping the application.

► *To stop the application manually:*

1. Right-click to bring up the context menu of the application icon (see page [23](#)) that is located in the taskbar notification area.
2. In the context menu, select **Exit**.

Kaspersky Security needs to be started manually if you have previously disabled automatic startup of the application (see section "Enabling and disabling automatic startup of the application" on page [26](#)).



► *To start the application manually,*

in the **Start** menu, select **Programs** → **Kaspersky Security for Virtualization 4.0 Light Agent**.

Pausing and resuming virtual machine protection and control

Pausing virtual machine protection and control means disabling all protection and control components of Kaspersky Security for a certain amount of time.

Application status is indicated by the application icon in the task bar notification area (see section "Application icon in the task bar notification area" on page [21](#)).

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

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

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

► *To pause or resume virtual machine protection and control:*

1. To pause virtual machine 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** window opens.

c. Select one of the following options:

- **Pause for the specified time** – Virtual machine 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** – Virtual machine 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** – Virtual machine protection and control resume when you decide to re-enable them.

2. If you decide to resume virtual machine protection and control, you can do so at any time, regardless of the virtual machine protection and control pause option that you selected previously. To resume virtual machine 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**.

Virtual machine protection state

This section describes ways to detect security threats and configure protection against them.



In this section:

Virtual machine protection status indication.....	29
Resolving virtual machine protection problems	31

Virtual machine protection status indication

Kaspersky Security reports events that reflect the current virtual machine protection status by means of various methods of indication in the main application window.

Kaspersky Security uses the following methods of virtual machine protection status indication:

- Indication by means of Kaspersky Security component operation status icons and component states. The following indication options are possible:
 - A green icon  of component operation status is displayed in the line of an enabled component. Statistics on the number of objects scanned and threats detected by this component, and the actions taken by this component in response to threats are displayed on the right.
 - A yellow icon  of component operation status is displayed in the line of a disabled component. In this case, component operation statistics are not displayed.
 - If all control components or protection components are disabled, the header of the **Endpoint control** or **Manage protection** section shows the status as *disabled*.
 - If one or several control components or protection components are enabled, the header of the **Endpoint control** or **Manage protection** section displays the status as *partly enabled (operating components: <number of enabled components in the section> out of <the total number of components in the section>)*.

- Indication of threats detected by Kaspersky Security components (for example, *application startups allowed, application startups blocked, objects scanned, threats detected*):
 - If the **Endpoint control** or **Manage protection** section is minimized, threats are indicated in the line with general operation statistics of components under the section header.
 - If the **Endpoint control** or **Manage protection** section is maximized, threats are indicated in the line with operation statistics of each component.

Depending on the threat type, information about the threat and its importance level is recorded as an event and displayed on one of the tabs in the **Reports and Storages** window:

- **Reports.**
- **Backup.**
- **Unprocessed files.**
- Indication using notifications about events in the operation of Kaspersky Security protection components relating to the status of a protected virtual machine (for example: *Virtual machine needs rebooting* or *No connection to SVM*). The messages are displayed as follows:
 - When the **Manage protection** section is minimized, the message is displayed instead of the line with statistics under the section header.
 - When the **Manage protection** section is maximized, the message is displayed instead of the line with statistics of the File Anti-Virus component.
- Indication by means of messages about events relating to Kaspersky Security tasks or abnormal operation of the application (for example: *databases and application modules are obsolete*). The messages are displayed as follows:
 - When the **Tasks** section is minimized, messages are displayed in the information space under the section header.
 - If the **Tasks** section is maximized, messages are displayed instead of the line with statistics and the schedule of the update task.
- Indication by means of messages about licensing problems.

If there are licensing problems (such as an expired license), they are indicated by means of messages highlighted in red in the **Licensing** window that opens when you click the **License** link located at the bottom of the main application window.

Resolving virtual machine protection problems

You can resolve virtual machine protection problems in one of the following ways:

- Resolve the problem right away. On seeing information about critical and important events relating to the virtual machine protection status, you can get right to fixing the problem:
 - If an application component has detected virtual machine security problems, you can click the **Reports** item in the context menu of the component to view information about files in which Kaspersky Security has detected the threat and select an action to perform on such files (for example, delete the files or restore them to the original folder).
 - If the virtual machine needs rebooting, you can exit all applications and restart the virtual machine.
 - If databases and application modules are outdated, you can start the update task.
 - If there are licensing problems, a relevant message is displayed in the **Licensing** window that opens when you click the **License** link located at the bottom of the main application window. Contact the administrator to resolve the licensing problem.
- Postpone problem resolution. If the problem cannot be resolved right away for any reason, you can postpone resolving the problem and return to it later.

Serious problems cannot be postponed. Examples of such problems include malfunctions of one or several application components, corrupted application files, or an expired license.

Connection of a protected virtual machine to an SVM

This section provides information on the specifics of connecting a protected virtual machine to an SVM.

In this section:

About connecting a protected virtual machine to an SVM.....	32
Configuring SVM discovery settings.....	33

Connecting a protected virtual machine to an SVM

In order for the application to work, the protected virtual machine has to be connected to an SVM with Protection Server installed.

If the protected virtual machine is not connected to any of the SVMs, the application does not scan files on the protected virtual machine. Files that must be scanned according to the protection settings are sent for scanning after a connection to the SVM is established.

To be able to select an SVM to connect to, the protected virtual machine has to receive information about SVMs available on the network. The protected virtual machine selects an SVM to which an optimal connection can be established according to the SVM selection algorithm.

See the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent* for details on connecting a protected virtual machine to an SVM.

You can configure the SVM discovery settings that are used by the protected virtual machine (see section "Configuring SVM discovery settings" on page [33](#)).

Configuring SVM discovery settings

► *To configure the settings for discovering SVMs operating on the network, and to receive information about them:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Advanced Settings** section, select **SVM discovery settings**.

SVM discovery settings will appear in the right part of the window.

3. Select the way in which the protected virtual machine will detect SVM and receive information about it:

- **Use Multicast.**

If this option is selected, the Light Agent component uses Multicast to receive information about SVMs.

This option is selected by default.

- **Use Integration Server.**

If this option is selected, the protected virtual machine connects to the Integration Server to receive a list of SVMs available for connection and information about them. If you want to use the Integration Server, you have to specify the settings of protected virtual machine connection to the Integration Server.

- **Use the custom list of SVM addresses.**

If this option is selected, you can specify the list of SVMs to which the protected virtual machine can connect.

4. If the **Use Integration Server** option is selected, specify the settings that control how the protected virtual machine connects to the Integration Server. To do so:
 - a. By default, the **Address** field shows the domain name of the computer hosting the Administration Console of Kaspersky Security Center. If this computer does not belong to a domain or if the Integration Server is installed on a different computer and the field shows the wrong address, specify the IP address in IPv4 format or the fully qualified domain name (FQDN) of the Integration Server.
 - b. If the port for connecting to the Integration Server differs from the default port (7271), specify the port number in the **Port** field.
 - c. If the computer hosting the Kaspersky Security Center Administration Console does not belong to a domain or your domain account does not belong to the KLAdmins group or to the group of local administrators, the **Connection to Integration Server** window opens. Specify the password of the Integration Server administrator (password of the admin account). A connection to the Integration Server under the administrator account is needed to receive from the Integration Server the settings of the account under which the protected virtual machine connects to the Integration Server.

After the settings that control how information about SVMs is received have been saved, the connection to the Integration Server is tested. If the connection test failed or the connection to the Integration Server could not be established, check the specified connection settings. Information about Integration Server connection errors is saved in the Integration Server operation log. You can view the Integration Server log in the Integration Server Management Console (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

5. If the **Use the custom list of SVM addresses** option is selected, create a list of SVMs. To do so:
 - a. Click the **Add** button located above the list of SVM addresses.

The **SVM addresses** window opens.
 - b. Enter the IP address in IPv4 format or the fully qualified domain name (FQDN) of the SVM to which the protected virtual machine can connect. You can enter several IP addresses or full domain names of the SVMs by typing them from a new line.

In the list of SVM addresses, specify only full domain names (FQDN) that are matched by a single IP address. Using a full domain name matched by several IP addresses can cause application errors.

- c. In the **SVM Addresses** window, click **OK**.

The specified addresses and fully qualified domain names of SVMs are checked. If some addresses or names are not recognized, a relevant message with the number of addresses or names that have not been recognized appears in a separate window. Recognized addresses and fully qualified domain names appear in the list of addresses of SVMs.

- d. To remove an IP address or fully qualified domain name of an SVM from the list, select it in the list and click the **Delete** button above the list.

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

Protecting the file system of a virtual machine. 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	36
Enabling and disabling File Anti-Virus	37
Configuring File Anti-Virus.....	38

About File Anti-Virus

File Anti-Virus prevents infection of the protected virtual machine's file system. By default, File Anti-Virus starts together with Kaspersky Security, continuously remains active in virtual machine memory, and scans all files that are opened, saved, or executed on the protected virtual machine for viruses and other malware.

File Anti-Virus uses the signature and heuristic analysis methods, and also iSwift technology. Before scanning a file, File Anti-Virus checks whether the iSwift databases contain information about this file, and uses this information to decide whether or not the file needs scanning. If the scan does not detect viruses or other malware in the file, Kaspersky Security grants access to the file.

If File Anti-Virus detects a threat in the file during scanning, Kaspersky Security assigns one of the following status labels to this file to designate the type of object detected (for example: *virus*, *Trojan program*).

The application then displays a notification about the threat that is detected in the file (if this is specified in the notification settings), and performs the action that is specified in the settings of File Anti-Virus on the file.

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.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
- From the application settings window (see section "Application settings window" on page [25](#)).



► *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. Open the **Manage protection** section.
4. Right-click to bring up the context menu of the **File Anti-Virus** 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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► 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 File Anti-Virus component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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.

Configuring File Anti-Virus

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

- Configure File Anti-Virus to be paused automatically according to schedule or at application startup.
- 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 application 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 can detect new malicious objects for which there are currently no records in the application database.

- Configure the use of iSwift scanning technology.

You can enable the use of the iSwift technology, which optimizes the speed of file scanning by excluding files that have not been modified since the most recent scan. iSwift technology also involves using SharedCache technology that optimizes the speed of file scanning by excluding files that have been already checked on a different virtual machine from scanning.

- Optimize scanning.

You can optimize the scanning of files by File Anti-Virus: shorten the scan duration and speed up Kaspersky 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:

Automatically pausing File Anti-Virus	40
Changing the file security level.....	41
Changing the File Anti-Virus action to take on infected files	42
Editing the protection scope of File Anti-Virus	43
Configuring the usage of Heuristic Analyzer with File Anti-Virus.....	45
Configuring the usage of iSwift technology in the operation of File Anti-Virus.....	46
Optimizing file scanning by File Anti-Virus.....	47
Scanning of compound files by File Anti-Virus.....	47
Changing the scan mode	49

Automatically pausing File Anti-Virus

You can configure the File Anti-Virus 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, please contact Kaspersky Lab Technical Support (http://support.kaspersky.com/#s_tab4).

► To configure automatic pausing of File Anti-Virus:

1. Open the application settings window (see page [25](#)).
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 File Anti-Virus component's settings 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 operation** section, do the following:

- 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 operation** 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 operation** 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.

Changing the file security level

To protect the virtual machine's file system, File Anti-Virus applies various groups of settings.

These groups of settings are called *file security levels*. There are three 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 (see page [25](#)).
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 File Anti-Virus component's settings 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 your 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 File Anti-Virus action to take on infected files

► *To change the File Anti-Virus action to take on infected files:*

1. Open the application settings window (see page [25](#)).
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 File Anti-Virus component's settings are displayed.

3. In the **Action on threat detection** section, select the required option:

- **Select action automatically.**

This option is selected by default. On detecting a threat the application performs the action **Disinfect. Delete if disinfection fails**.

- **Perform action: Disinfect. Delete if disinfection fails.**
- **Perform action: Disinfect.**

Regardless of the option selected, Kaspersky Security applies the **Delete** action to files that are part of the Windows Store application.

- **Perform action: Delete.**
- **Perform action: Block.**

When they are deleted or disinfected, copies of files are saved in Backup.

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 during its operation. 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, removable drives, and network drives of a virtual machine.

► *To create the protection scope of File Anti-Virus:*

1. Open the application settings window (see page [25](#)).
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 File Anti-Virus component's settings 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 **General** tab.

5. In the **File types** section, specify the type of files that you want File Anti-Virus to scan:

- 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 can send a virus or other malware to your virtual machine in an executable file that has had its extension changed to .txt. 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 **Protection scope** section, do one of the following:

- To add a new object to the list of objects to be scanned, click the **Add** button.

The **Select object** window opens.

- If you want to change the path to an object, select one from the list of objects and click the **Edit** button.

The **Select object** window opens.

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

A window for confirming deletion opens.

7. In the **Select object** window, do one of the following:

- If you want to add a new object, select one in the **Select object** window and click the **Add** button.

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

Click **OK**.

- To change the path to an object in the list of objects, enter a different path to the object in the **Object** field and click **OK**.
- If you want to remove an object, click the **Yes** button in the window for confirming removal.

8. If necessary, repeat steps 6 and 7 to add objects, change the path to objects, or remove objects from the protection scope.

9. If you want to exclude an object from the protection scope, clear the check box next to the object in the **Protection scope** list. The object remains on the list of objects to be scanned, though it is excluded from scanning by File Anti-Virus.

10. Click **OK** in the **File Anti-Virus** window.

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

Configuring the usage of 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 (see page [25](#)).

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 File Anti-Virus component's settings 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, do one of the following:
 - 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: **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.

Configuring the usage of iSwift technology in the operation of File Anti-Virus

► *To configure the usage of iSwift technology in the operation of File Anti-Virus:*

1. Open the application settings window (see page [25](#)).
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 File Anti-Virus component's settings 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 **Scanning technology** section, do one of the following:
 - Select the **iSwift technology** check box to use File Anti-Virus with this technology enabled.
 - Clear the **iSwift technology** check box to use File Anti-Virus with this technology disabled.

Enabling the iSwift technology also enables the SharedCache technology.

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

Optimizing file scanning by File Anti-Virus

► *To optimize file scanning:*

1. Open the application settings window (see page [25](#)).
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 File Anti-Virus component's settings are displayed.

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

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

4. 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 of compound files by File Anti-Virus

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 (see page [25](#)).
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 File Anti-Virus component's settings 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 **Performance** tab, in the **Scan of compound files** section, specify the types of compound files that you want to scan: archives, installation packages, or embedded OLE objects by selecting the corresponding check boxes.
5. 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 set, only new files are scanned.

6. Click the **Additional** button.

The **Compound files** window opens.

7. In the **Background scan tasks** 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.

8. 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 set.

9. In the **Compound files** window, click **OK**.

10. Click **OK** in the **File Anti-Virus** window.

11. 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 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 you, by an application on behalf of you or a different user (under the account credentials that were used to log in to the operating system), or by the operating system. For example, when a Microsoft Office Word document is used, Kaspersky 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 (see page [25](#)).

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 File Anti-Virus component's settings 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.

Email protection. Mail Anti-Virus

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system.

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


In this section:

About Mail Anti-Virus.....	50
Enabling and disabling Mail Anti-Virus	51
Configuring Mail Anti-Virus.....	53

About Mail Anti-Virus

Mail Anti-Virus scans incoming and outgoing email messages (hereinafter also "messages" or "mail") for viruses and other malware. It starts together with Kaspersky Security, continuously remains active in virtual machine memory, and scans all messages that are sent or received via the POP3, SMTP, IMAP, and NNTP protocols.

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

Mail Anti-Virus status is indicated by the application icon in the task bar notification area (see section "Application icon in the taskbar notification area" on page [21](#)). The application icon appears as  every time an email message is scanned if application icon animation is enabled (see section "Enabling and disabling the animation of the application icon" on page [22](#)).

Mail Anti-Virus intercepts and scans each email message that you receive or send. If no threats are detected in the message, it becomes available to the user.

If Mail Anti-Virus detects a threat in the message during scanning, Kaspersky Security assigns one of the following status labels to this message to designate the type of object detected (for example: *virus*, *Trojan program*).

The application then blocks the email message, displays an on-screen notification (if configured to do so in the notification settings) about the detected threat, and performs the action on the message according to the settings of Mail Anti-Virus (see section "Changing the action to take on infected email messages" on page [55](#)).

A plug-in is available for the Microsoft Office Outlook application, which allows fine-tuning the message scan settings. The Mail Anti-Virus plug-in is embedded in the Microsoft Office Outlook application during installation of Kaspersky Security.

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.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
 - From the application settings window (see section "Application settings window" on page [25](#)).
- *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. Open the **Manage protection** section.
 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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *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 Mail Anti-Virus component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 mail security level.

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

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

- Change the action that Kaspersky Security performs on an infected email message.
- Edit the protection scope of Mail Anti-Virus.
- Configure scanning of objects attached to messages.

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

- Configure filtering by the type of attachment to email messages.

Filtering of message attachments by type allows files of the specified types to be automatically renamed or deleted. By renaming an attachment of a certain type, Kaspersky Security can protect your virtual machine against automatic execution of malware.

- Configure Heuristic Analyzer.

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

- Configure email scanning in Microsoft Office Outlook.

An embeddable plug-in is available for the Microsoft Office Outlook application, which allows adjusting email scan settings.

When you use other applications, 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 you use Mozilla Thunderbird, Mail Anti-Virus does not scan messages that are transmitted via the IMAP protocol for viruses and other malware if filters are used that move messages from the Inbox folder.

In this section:

Changing the mail security level.....	54
Changing the action to take on infected email messages.....	55
Editing the protection scope of Mail Anti-Virus	56
Filtering attachments in messages	59
Using Heuristic Analyzer with Mail Anti-Virus	60
Scanning emails in Microsoft Office Outlook	60

Changing the mail security level

Mail Anti-Virus applies various groups of settings to protect mail. The settings groups are called *mail security levels*. There are three mail 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 mail security level:

1. Open the application settings window (see page [25](#)).
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 Mail Anti-Virus component's settings are displayed.

3. In the **Security level** section, do one of the following:
 - If you want to install one of the pre-installed mail security levels (**High**, **Recommended**, or **Low**), use the slider to select one.

- If you want to configure a custom mail security level, click the **Settings** button and specify settings in the **Mail Anti-Virus** window.

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

- If you want to change the mail 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 (see page [25](#)).
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 Mail Anti-Virus component's settings are displayed.

3. In the **Action on threat detection** section, select the action that Kaspersky Security performs on detecting an infected email message:

- **Select action automatically.**
- **Perform action: Disinfect. Delete if disinfection fails.**
- **Perform action: Disinfect.**
- **Perform action: Delete.**
- **Perform action: Block.**

The default selection is **Perform action: Disinfect. Delete if disinfection fails**.

When they are deleted or disinfected, copies of messages are saved in Backup.

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 during its operation. The protection scopes of different components have different properties. The properties of the protection scope of Mail Anti-Virus include the settings of Mail Anti-Virus integration into email clients, and the type of email messages and the email protocols whose traffic is scanned by Mail Anti-Virus. By default, Kaspersky Security scans both incoming and outgoing messages and traffic via the POP3, SMTP, IMAP, and NNTP protocols, and is integrated into the Microsoft Office Outlook application.

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

1. Open the application settings window (see page [25](#)).
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 Mail Anti-Virus component's settings 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 **General** tab.
5. In the **Protection scope** section, do one of the following:

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

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

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

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

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

If you use an email client other than Microsoft Office Outlook, messages that are transmitted via the POP3, SMTP, NNTP and IMAP protocols are not scanned by Mail Anti-Virus when the **POP3 / SMTP / NNTP / IMAP traffic** check box is cleared.

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

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

Clear the **Additional: Microsoft Office Outlook plug-in** check box if you want to block access to Mail Anti-Virus settings from Microsoft Office Outlook and disable scanning of the messages that are transmitted via the POP3, SMTP, NNTP, and IMAP protocols after they arrive on the virtual machine by a plug-in that is embedded into Microsoft Office Outlook.

The Mail Anti-Virus plug-in is embedded in the Microsoft Office Outlook application during installation of Kaspersky Security.

7. Click **OK**.

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

► *To configure the scanning of objects attached to email messages:*

1. Open the application settings window (see page [25](#)).

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 Mail Anti-Virus component's settings are displayed.

3. Click the **Settings** button.

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

4. In the **Mail Anti-Virus** window, select the **General** tab.

5. Perform the following in the **Scan of compound files** section:

- If you want Mail Anti-Virus to skip archives that are attached to messages, clear the **Scan attached archives** check box.
- If you want Mail Anti-Virus to skip message attachments that are larger than N megabytes in size, set the **Do not scan archives larger than N MB** check box. If you set 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 skip message attachments that take more than N seconds to scan, set the **Do not scan archives for more than N sec** check box. If you set this check box, specify the maximum archive scan time in the field that is opposite the name of the check box.

6. Click **OK**.

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

Filtering attachments in messages

Malicious programs can be distributed in the form of message attachments. You can configure filtering of email message 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 (see page [25](#)).
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 Mail Anti-Virus component's settings 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 message attachments, select the **Disable filtering** option.
- If you want Mail Anti-Virus to rename message attachments of the specified types, select the **Rename specified attachment types** option.
- If you want Mail Anti-Virus to delete message attachments of the specified types, select the **Delete specified attachment types** option.

6. If in step 5 of these instructions you have selected the **Rename specified attachment types** option or the **Delete specified attachment types** option, the list of file types becomes active. Set 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 Analyzer with Mail Anti-Virus

► *To configure the use of Heuristic Analyzer in the operation of Mail Anti-Virus:*

1. Open the application settings window (see page [25](#)).
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 Mail Anti-Virus component's settings 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. In the **Scan methods** section:

- If you want Mail Anti-Virus to use heuristic analysis, select the **Heuristic Analysis** check box and use the slider to set the level of heuristic analysis: **light scan**, **medium scan**, or **deep scan**.
- If you do not want Mail Anti-Virus to use heuristic analysis, clear the **Heuristic Analysis** check box.

6. Click **OK**.

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

Scanning emails in Microsoft Office Outlook

During installation of Kaspersky Security, a special plug-in is embedded into Microsoft Office Outlook. It allows you to open the Mail Anti-Virus settings 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, and IMAP protocols.

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

In Microsoft Office Outlook, incoming messages are first scanned by Mail Anti-Virus (when the **POP3 / SMTP / NNTP / IMAP traffic** check box is set in the interface of Kaspersky Security) and then scanned 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.

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

Your choice of action in the notification window determines the component that eliminates the threat in the 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.

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

1. Open the main Microsoft Outlook application window.
2. Select **Service** → **Settings** option from the menu bar.

The **Settings** window opens.

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

Protecting virtual machine web traffic. Web Anti-Virus

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system.

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

In this section:

About Web Anti-Virus.....	62
Enabling and disabling Web Anti-Virus.....	63
Configuring Web Anti-Virus.....	65

About Web Anti-Virus

Every time you go online, you expose information that is stored on your virtual machine to viruses and other malware. They can infiltrate your virtual machine while you are downloading free software or browsing websites that are compromised by hacker attacks. Network worms can find a way onto your virtual machine 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 virtual machine over the HTTP and FTP protocols and checks links against the list of malicious or phishing web addresses.

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

- If the page or file is found not to contain malicious code, the user gains immediate access to them.
- If the web page or the file contains malicious code, the application takes the action on the object that is specified in the settings of Web Anti-Virus (see section "Changing the action to take on malicious web traffic objects" on page [67](#)).

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.



You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
 - From the application settings window (see section "Application settings window" on page [25](#)).
- *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. Open the **Manage protection** section.
 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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *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 Web Anti-Virus component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 Security performs on malicious 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 to check links against databases of phishing and malicious web addresses.
- 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 Security analyzes the activity of applications in the operating system. Heuristic analysis can detect new malicious objects for which there are currently no records in the Kaspersky Security database.

- Configure use of heuristic analysis when scanning web pages for phishing links.
- Optimize traffic scanning by Web Anti-Virus.

To optimize web traffic scanning, you can configure the duration of inbound and outbound HTTP and FTP traffic caching by Web Anti-Virus.

- Create a list of trusted web addresses.

You can create a list of web addresses whose content you trust. Web Anti-Virus does not analyze information from trusted web addresses 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 web address may be the address of a specific web page or the address of a website.

In this section:

Changing the web traffic security level	66
Changing the action to take on malicious web traffic objects	67
Web Anti-Virus scanning of URLs against databases of phishing and malicious web addresses	67
Using Heuristic Analyzer with Web Anti-Virus	69
Configuring the duration of caching web traffic	69
Editing the list of trusted web addresses	71

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 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 (see page [25](#)).
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 Web Anti-Virus component's settings 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 (see page [25](#)).
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 Web Anti-Virus component's settings are displayed.

3. In the **Action on threat detection** section, select the action that Kaspersky Security performs on malicious web traffic objects:

- **Select action automatically.**
- **Block download.**
- **Allow download.**

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

Web Anti-Virus scanning to check links against databases of phishing and malicious web addresses

Scanning links to see if they are included in the list of phishing web addresses allows *phishing attacks* to be avoided. 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. The link takes you to an exact copy of the bank's website and you can even see the address of the bank's original website in the browser. However, you are actually on a counterfeit website. From this point forward, all of your actions 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 while scanning web traffic and blocks access to such sites. Lists of phishing web addresses are included in the Kaspersky Security distribution kit and are updated as updated lists become available in the application databases.

► *To configure Web Anti-Virus to check links against the databases of phishing and malicious web addresses:*

1. Open the application settings window (see page [25](#)).
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 Web Anti-Virus component's settings 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. Do the following:

- If you want Web Anti-Virus to check links against the databases of malicious web addresses, in the **Scan methods** section, select the **Check if links are listed in the database of malicious web addresses** check box.
- If you want Web Anti-Virus to check links against the databases of phishing web addresses, in the **Anti-Phishing Settings** section, select the **Check if links are listed in the database of phishing URLs** check box.

You can also use the reputation databases of Kaspersky Security Network to check links against the databases of phishing and malicious web addresses.

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 (see page [25](#)).
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 Web Anti-Virus component's settings 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. Do the following:

- If you want Web Anti-Virus to use heuristic analysis to scan web traffic for viruses and other malware, in the **Scan methods** section, select the **Heuristic analysis for detecting viruses** check box and use the slider to set the level 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, in the **Anti-Phishing Settings** section, select the **Heuristic analysis for detecting phishing links** check box and use the slider to set the level 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 protected virtual machine in full.

Caching 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 reduces the time that is needed to deliver objects to the user and eliminates the connection loss problem. The Internet security level is not reduced in that case.

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

► *To configure web traffic caching time:*

1. Open the application settings window (see page [25](#)).
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 Web Anti-Virus component's settings 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 **Actions** 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 web addresses

► To create a list of trusted web addresses:

1. Open the application settings window (see page [25](#)).
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 Web Anti-Virus component's settings are displayed.

3. Click the **Settings** button.

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

4. Select the **Trusted web addresses** tab.
5. Select the **Do not scan web traffic from trusted web addresses** check box.
6. Create a list of addresses of websites / 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 web addresses.

- d. If necessary, repeat steps a–c of the instructions.
7. Click **OK**.
 8. To save changes, click the **Save** button.

Protection of IM client traffic.

IM Anti-Virus

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system.

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

In this section:

About IM Anti-Virus	72
Enabling and disabling IM Anti-Virus	73
Configuring IM Anti-Virus	75

About IM Anti-Virus

IM Anti-Virus is designed to scan traffic transmitted by IM clients.

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

- Links that, when clicked, lead to attempts to download malware to the virtual machine.
- Links to malicious programs and websites that intruders use for phishing attacks.

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

Files can be transmitted through IM clients. When you attempt to save such files, they are scanned by the File Anti-Virus component (see section "About File Anti-Virus" on page [36](#)).

IM Anti-Virus intercepts every message that the user sends or receives through an IM client and scans it for links that may threaten virtual machine security.

The following happens next:

- If no malicious links are detected in the message, it becomes available to the user.
- If dangerous links are detected in the message, IM Anti-Virus replaces the message with information about the threat in the message window of the active IM client.

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.

You can enable or disable a component in two ways:


- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
 - From the application settings window (see section "Application settings window" on page [25](#)).
- *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. Open the **Manage protection** section.
 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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable IM 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 the **IM Anti-Virus** section.

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

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 links in IM client messages against databases of malicious and phishing web addresses.
- Configure Heuristic Analyzer.

To increase the effectiveness of protection, you can use heuristic analysis. During heuristic analysis, Kaspersky 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 Security databases.

In this section:

Creating the protection scope of IM Anti-Virus	75
Scanning URLs against databases of malicious and phishing web addresses with IM Anti-Virus	76
Using Heuristic Analyzer with IM Anti-Virus.....	77

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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select the **IM Anti-Virus** section.

In the right part of the window, the IM Anti-Virus component's settings 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 scan only incoming IM client messages, select the **Incoming messages only** option.
4. To save changes, click the **Save** button.

Scanning links against databases of malicious and phishing web addresses with IM Anti-Virus

► *To configure IM Anti-Virus to check links against the databases of malicious and phishing web addresses:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select the **IM Anti-Virus** section.

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

3. In the **Scan methods** section, select the methods that you want IM Anti-Virus to use:
 - If you want to check links in IM client messages against the database of malicious web addresses, select the **Check if links are listed in the database of malicious web addresses** check box.

- If you want to check links in IM client messages against the database of phishing web addresses, select the **Check if links are listed in the database of phishing web addresses** 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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select the **IM Anti-Virus** section.

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

3. In the **Scan methods** section:
 - a. Select the **Heuristic analysis** check box.
 - b. Use the slider to set the level 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, Network Attack Blocker, and Network Monitor components, and of network traffic control.

In this section:

Firewall	78
Network Attack Blocker	109
Monitoring network traffic	112
Network Monitor	117

Firewall

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

In this section:

About Firewall	79
Enabling or disabling Firewall.....	80
About network rules	82
About the network connection status.....	83
Changing the network connection status.....	84
Managing network packet rules.....	84
Managing network rules for application groups	91
Managing network rules for applications	100

About Firewall

During use on LANs and the Internet, your virtual machine 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 your protected virtual machine, blocking network threats while the virtual machine is connected to the Internet or a local area network.

Firewall detects all network connections of your virtual machine and provides a list of IP addresses, with an indication of the status of the default network connection.

When a remote connection to a protected virtual machine is established after installation of the application, Firewall is enabled by default, blocking the RDP session. To prevent the session from being blocked, change the Firewall action (see section "Changing the Firewall action for a network packet rule" on page [90](#)) for the "Remote desktop network activity" network packet rule to **Allow**.

The Firewall component filters all network activity according to network rules (see section "About network rules" on page [82](#)). Configuring network rules lets you specify the desired level of virtual machine protection, from blocking Internet access for all applications to allowing unlimited access.

When working with the Firewall, please keep in mind the following special considerations:

- Network activity at the application level via the TCP and UDP protocols is not blocked if the IP address of the sender matches the IP address of the recipient, under the condition that the packet was sent via RAW socket.
- The Firewall does not check the application rules and allows network activity if the remote computer has the following IP address:
 - for IPv4: 127.0.0.1
 - for IPv6: ::1under the condition that the packet was sent via RAW socket.
- The local address from which/to which data is sent may be undefined in the following cases:
 - The application that initiated the network activity via the TCP or UDP protocols did not specify a local IP address.
 - The application initiated the network activity via the ICMP protocol.

- The application receives an incoming packet via the UDP protocol.
- The Firewall does not filter loopback traffic at the network level. Decisions on loopback packets are made at the application level.
- When filtering network activity at the application level via the ICMP protocol, the Firewall supports only an outgoing ICMP Echo-Request.
- There is no filtering of incoming ICMP packets at the application level.
- For outgoing network activity via RAW socket, there is no filtering based on packet rules at the application level.
- Packets that are filtered out by the Network Attack Blocker component are not scanned by the Firewall.
- If a virtual machine has tunneling network interfaces, filtering of tunneling traffic based on packet rules is repeated for the same packet as the packet propagates between interfaces.

Enabling or disabling Firewall

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



You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
 - From the application settings window (see section "Application settings window" on page [25](#)).
- *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. Open the **Manage protection** section.



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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable Firewall, in 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 **Firewall**.

In the right part of the window, the Firewall component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. Do one of the following:

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

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

About network rules

Network rule is an allowed or blocked action that is 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 application 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 applications installed on your virtual machine 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.

The rules for controlling the network activity of applications do not take into account the following filter settings specified at the network level:

- Network adapter ID
- List of MAC addresses of the local adapter
- List of local MAC addresses

- Remote MAC addresses list
- Type of Ethernet frame (IP, IPv6, ARP)
- Time to live (TTL) of the IP packet

As a result of the joint use of rules by the network level and application level, network traffic may be blocked at the application level even if it is allowed at the network level.

You can specify an execution priority for each network packet rule (see section "Changing the priority of a network packet rule" on page [90](#)) and each network rule for applications (see section "Changing the priority of an application network rule" on page [108](#)).

About the network connection status

Firewall controls all network connections on your virtual machine 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 virtual machine that is connected to such a network, Firewall blocks access to files and printers of this virtual machine. External users are also unable to access data through shared folders and remote access to the desktop of this virtual machine. 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 your virtual machine (for example, a LAN or home network).
- **Trusted network.** This status is intended for a safe network in which the virtual machine 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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.
In the right part of the window, the Firewall component's settings are displayed.
3. Click the **Available networks** button.
The **Firewall** window opens.
4. Select the **Networks** tab.
5. Select a network connection whose status you want to change.
6. Right-click to display the context menu of the network connection.
7. In the context menu, select network connection status (see section "About the network connection status" on page [83](#)):
 - **Public network.**
 - **Local network.**
 - **Trusted network.**
8. In the **Firewall** window, click **OK**.
9. 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.

- Delete 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.....	85
Enabling or disabling a network packet rule	89
Changing the Firewall action for a network packet rule	90
Changing the priority of a network packet rule.....	90

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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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 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 Firewall should monitor 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 set 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 (packet).**
- **Inbound.**
- **Inbound / Outbound.**
- **Outbound (packet).**
- **Outbound.**

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 your virtual machine 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 your virtual machine in the **Local ports** field.
12. In the **Network adapters** table, specify the settings of network adapters from which network packets can be sent or which can receive network packets. To do so, use the **Add**, **Edit**, and **Delete** buttons.
13. In the **Maximum value of packet time to live** field, specify the range of values of the time to live for inbound and/or outbound network packets. A network rule controls the transmission of network packets whose time to live is within the range from 1 to the specified value.
14. Specify the network addresses of remote computers that can send and/or receive network packets. To do so, select one of the following values in the **Remote addresses** drop-down list:
 - **Any address.** The network rule controls network packets sent and/or received by remote computers with any IP address.
 - **Subnet addresses.** The network rule controls network packets sent and/or received by remote computers with IP addresses associated with the selected network type: **Trusted networks, Local networks, Public networks.**
 - **Addresses from a list.** The network rule controls network packets sent and/or received by remote computers with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.
15. Specify the network addresses of virtual machines with Kaspersky Security installed, which can send and/or receive network packets. To do so, select one of the following values in the **Local addresses** drop-down list:
 - **Any address.** The network rule controls network packets sent and/or received by virtual machines with Kaspersky Security installed and with any IP address.
 - **Addresses from a list.** The network rule controls network packets sent and/or received by virtual machines with Kaspersky Security installed and with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.

Sometimes the local address cannot be obtained for applications. In this case, the **Local addresses** setting is ignored.

16. If you want the actions of the network packet rule to be reflected in the report, select the **Log event** check box.

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

If you create a new network packet 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.

18. In the **Firewall** window, click **OK**.

19. 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 (see page [25](#)).

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

In the right part of the window, the Firewall component's settings 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, set 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. In the **Firewall** window, click **OK**.

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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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 application rule.**
- **Log events.**

6. In the **Firewall** window, click **OK**.

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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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 **Move up** and **Move down** buttons to move the network packet rule to the desired spot in the list of network packet rules.
6. In the **Firewall** window, click **OK**.
7. To save changes, click the **Save** button.

Managing network rules for application groups

By default, Kaspersky Security groups all applications that are installed in the operating system of the protected virtual machine 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.

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 section "About Application Privilege Control" on page [138](#)). 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 Security on the virtual machine. 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.

- Delete 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	97
Changing the Firewall action for an application group network rule	98
Changing the priority of an application group network rule	99

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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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. 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 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 for which Firewall should monitor 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 set 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 / Outbound.**
- **Outbound.**

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 your virtual machine and the remote computer 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 your virtual machine in the **Local ports** field.

15. In the **Maximum value of packet time to live** field, specify the range of values of the time to live for inbound and/or outbound network packets. A network rule controls the transmission of network packets whose time to live is within the range from 1 to the specified value.

16. Specify the network addresses of remote computers that can send and/or receive network packets. To do so, select one of the following values in the **Remote addresses** drop-down list:

- **Any address.** The network rule controls network packets sent and/or received by remote computers with any IP address.
- **Subnet addresses.** The network rule controls network packets sent and/or received by remote computers with IP addresses associated with the selected network type: **Trusted networks, Local networks, Public networks.**

- **Addresses from a list.** The network rule controls network packets sent and/or received by remote computers with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.

17. Specify the network addresses of virtual machines with Kaspersky Security installed, which can send and/or receive network packets. To do so, select one of the following values in the **Local addresses** drop-down list:

- **Any address.** The network rule controls network packets sent and/or received by virtual machines with Kaspersky Security installed and with any IP address.
- **Addresses from a list.** The network rule controls network packets sent and/or received by virtual machines with Kaspersky Security installed and with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.

Sometimes the local address cannot be obtained for applications. In this case, the **Local addresses** setting is ignored.

18. If you want the actions of the network rule for a group of applications to be reflected in the report, select the **Log event** check box.

19. 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.

20. In the **Application group control rules** window, click **OK**.

21. In the **Firewall** window, click **OK**.

22. 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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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, set 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 (see page [25](#)).

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

In the right part of the window, the Firewall component's settings 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.

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

In the right part of the window, the Firewall component's settings 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 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 application group network rules that are created by default.

► *To change the priority of an application group network rule:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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 application group network rules, select the network rule whose priority you want to change.
8. Use the **Move up** and **Move 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 is detected by Kaspersky Security on the virtual machine. 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.

- Delete 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	102
Enabling or disabling an application network rule	105
Changing the Firewall action for an application network rule	106
Changing the priority of an application network rule	108

Creating and editing an application network rule

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

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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. 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 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 for which Firewall should monitor 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 set 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 / Outbound.**
- **Outbound.**

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 virtual machine 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 virtual machine in the **Local ports** field.

15. In the **Maximum value of packet time to live** field, specify the range of values of the time to live for inbound and/or outbound network packets. A network rule controls the transmission of network packets whose time to live is within the range from 1 to the specified value.

16. Specify the network addresses of remote computers that can send and/or receive network packets. To do so, select one of the following values in the **Remote addresses** drop-down list:

- **Any address.** The network rule controls network packets sent and/or received by remote computers with any IP address.
- **Subnet addresses.** The network rule controls network packets sent and/or received by remote computers with IP addresses associated with the selected network type: **Trusted networks, Local networks, Public networks.**
- **Addresses from a list.** The network rule controls network packets sent and/or received by remote computers with IP addresses that can be specified in the list below using the **Add, Edit, and Delete** buttons.

17. Specify the network addresses of virtual machines with Kaspersky Security installed, which can send and/or receive network packets. To do so, select one of the following values in the **Local addresses** drop-down list:

- **Any address.** The network rule controls network packets sent and/or received by virtual machines with Kaspersky Security installed and with any IP address.
- **Addresses from a list.** The network rule controls network packets sent and/or received by virtual machines with Kaspersky Security installed and with IP addresses that can be specified in the list below using the **Add**, **Edit**, and **Delete** buttons.

Sometimes the local address cannot be obtained for applications. In this case, the **Local addresses** setting is ignored.

18. If you want the actions of the network rule for an application to be reflected in the report, select the **Log event** check box.

19. 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.

20. In the **Application control rules** window, click **OK**.

21. In the **Firewall** window, click **OK**.

22. 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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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, set 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 (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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.

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 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 network rule

The priority of an application 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.

Application network rules (both inherited and custom) have a higher priority than network rules that are inherited from a parent application group. 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.

You cannot change the priority of inherited application network rules.

► *To change the priority of an application network rule:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Anti-Virus protection** section, select **Firewall**.

In the right part of the window, the Firewall component's settings 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 application network rule whose priority you want to edit.
8. Use the **Move up** and **Move 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.

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	110
Enabling and disabling Network Attack Blocker	110
Editing the settings used in blocking an attacking computer	112

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 the protected virtual machine, Kaspersky Security blocks network activity originating 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 section "Editing the settings used in blocking an attacking computer" on page [112](#)).

Descriptions of currently known types of network attacks and ways to fight them are provided in Kaspersky Security databases. The list of network attacks that are detected by Network Attack Blocker is updated during application database updates (see section "About database and application module updates" on page [212](#)).

Enabling and disabling Network Attack Blocker

By default, the Network Attack Blocker component is enabled and operating in optimal mode. You can disable Network Attack Blocker, if necessary.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
- From the application settings window (see section "Application settings window" on page [25](#)).


► *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. Open the **Manage protection** section.

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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable Network Attack Blocker in the application settings window:*

1. Open the application settings window.

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.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 (see page [25](#)).
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. Select the **Add the attacking computer to the list of blocked computers for N minutes** check box.

If this check box is set, 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 virtual machine 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 N minutes** check box.

By default, network traffic from the attacking computer is blocked for one hour.

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	113
Configuring the settings of network traffic monitoring	113

About network traffic monitoring

During the operation of Kaspersky Security, the Mail Anti-Virus (see section "About Mail Anti-Virus" on page [50](#)), Web Anti-Virus (see section "About Web Anti-Virus" on page [62](#)), and IM Anti-Virus (see section "About IM Anti-Virus" on page [72](#)) components monitor data streams that are transmitted via specific protocols and pass through open TCP and UDP ports of the virtual machine. For example, Mail Anti-Virus scans data that is transmitted via SMTP, while Web Anti-Virus scans data that is transmitted via HTTP and FTP.

Kaspersky 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.....	114
Creating a list of monitored network ports	114
Creating a list of applications for which all network ports are monitored.....	116

Enabling monitoring of all network ports

► To enable monitoring of all network ports:

1. Open the application settings window (see page [25](#)).
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 (see page [25](#)).
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 Security package.

5. In the list of network ports, perform the following:

- Set 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 set 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.

When the FTP protocol runs in passive mode, the connection can be established via a random network port that is not added to the list of monitored network ports. To protect such connections, you have to enable monitoring of all network ports (see section "Enabling monitoring of all network ports" on page [114](#)) or configure the monitoring of all ports for applications (see section "Creating a list of applications for which all network ports are monitored on page [116](#)) that establish the FTP connection.

Creating a list of applications for which all network ports are monitored

You can create a list of applications for which Kaspersky 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 Security monitors all network ports.

► *To create a list of applications for which all network ports are monitored:*

1. Open the application settings window (see page [25](#)).

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 specified applications** check box.

6. In the list of applications under the **Monitor all ports for specified applications** check box, do the following:

- Set the check boxes next to the names of applications for which you want to monitor all network ports.

By default, the check boxes are set 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 protected virtual machine, 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 it.

In this section:

About Network Monitor	117
Starting Network Monitor	118

About Network Monitor

Network Monitor is a tool designed for viewing information about the network activity of your virtual machine in real time.

Starting Network Monitor

► *To start Network Monitor:*

1. Open the main application window (see page [23](#)).
2. Select the **Protection and Control** tab.
3. Open the **Manage protection** section.
4. Right-click the **Firewall** line to open 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 protected virtual machine is shown on four tabs:

- The **Network activity** tab shows all current network connections with your protected virtual machine. Both outbound and inbound network connections of the protected virtual machine are displayed.
- The **Open ports** tab lists all open network ports of the protected virtual machine.
- The **Network traffic** tab shows the volume of inbound and outbound network traffic between the protected virtual machine and other computers in the network to which you are 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.

System Watcher

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system.

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

In this section:

About System Watcher.....	119
Enabling and disabling System Watcher	120
Using behavior stream signatures (BSS).....	122
Rolling back malware actions during disinfection	122

About System Watcher

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

Behavior stream signatures

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

Rolling back actions that have been performed by malware

Based on information that System Watcher collects, Kaspersky 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 section "Protecting the virtual machine file system. File Anti-Virus" on page [36](#)) and by Kaspersky Security during a virus scan.

Rolling back malware activity has no adverse effects on the operating system or the integrity of virtual machine data.

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 threats that they detect.



You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
 - From the application settings window (see section "Application settings window" on page [25](#)).
- *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. Open the **Manage protection** section.
 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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable System Watcher 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 **System Watcher**.

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

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 (see page [25](#)).
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 **System Watcher** component's settings are displayed.

3. In the **Proactive Defense** section, select the **Use behavior stream signatures (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 Security performs the default action that is specified by Kaspersky Lab specialists.
- **Terminate the malicious program.** If this item is selected, on detecting malicious activity Kaspersky Security terminates this application.
- **Skip.** If this item is selected, on detecting malicious activity Kaspersky 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 (see page [25](#)).
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 **System Watcher** component's settings are displayed.

3. Do one of the following:

- If you want Kaspersky 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 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.

Application Startup Control

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system and you selected "Standard installation" as the type of installation.

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

In this section:

About Application Startup Control	124
Enabling and disabling Application Startup Control	125
About Application Startup Control rules.....	127
About Application Startup Control operation modes	129
Managing Application Startup Control rules.....	130
Editing Application Startup Control message templates	137

About Application Startup Control

The Application Startup Control component monitors user attempts to start applications and regulates the startup of applications on the virtual machine by means of *Application Startup Control rules* (see section "*About Application Startup Control rules*" on page [127](#)).

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 attempts to start applications on the virtual machine are logged in reports.



Enabling and disabling Application Startup Control



Although Application Startup Control is enabled by default, you can disable Application Startup Control if necessary.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
 - From the application settings window (see section "Application settings window" on page [25](#)).
- *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. Open the **Endpoint control** section.
 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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable Application Startup 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 Startup Control.

In the right part of the window, the settings of the Application Startup Control component are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. In the **Application Control** section, 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.

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 Security does not restrict the startup of applications in accordance with the rule parameters, but only logs information about the startup of an application in a report.

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 *Test* status. Application allow and block settings are configured separately for test rules and non-test rules.

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 section "About Application Startup Control operation modes" on page [129](#)). 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 side of the Kaspersky Security administration plug-in. 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. Permission to run applications belonging to this KL category is required for the operation of Application Startup Control in White List mode" (see section "About Application Startup Control operation modes" on page [129](#)). This rule is created by default only on the side of the Kaspersky Security administration plug-in. The rule is disabled by default.

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 section "About Application Startup Control rules" on page [127](#)).

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 Application Startup Control allow rules are fully configured, Application Startup Control blocks all new applications not 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 Security local interface and Kaspersky Security Center. Since Kaspersky Security Center provides tools that are unavailable in the local interface of Kaspersky Security, it is recommended to configure the operating mode of the Application Startup Control component in Kaspersky Security Center (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*).

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.....	131
Adding a trigger condition for an Application Startup Control rule.....	132
Editing the status of an Application Startup Control rule	136

Adding and editing an Application Startup Control rule

► *To add or edit an Application Startup Control rule:*

1. Open the application settings window (see page [25](#)).
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.
 - If you want to edit a rule, select it in the list of rules and 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 or edit the list of inclusion conditions that trigger an Application Startup Control rule (see section "Adding a trigger condition for an Application Startup Control rule" on page [132](#)). To do so, use the **Add**, **Edit**, **Delete**, 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**, **Delete**, and **Convert into inclusion condition** 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 condition** 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 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 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 (see page [25](#)).
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 **Edit** button.

The **Application Startup Control rule** window opens.

4. Do one of the following:

- To add an inclusion condition, click the **Add** button in the **Inclusion conditions** table.
- To add an exclusion condition, click the **Add** button in the **Exclusion conditions** table.

The context menu of the **Add** button opens.

5. Do the following:

- To use the properties of the executable file of an application 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, File or folder path, File hash code (MD5)**, or **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, select the criterion based on which you want to create one or more conditions that trigger the rule: **Metadata**, **Folder path**, **File hash code (MD5)**, or **KL category** to which the executable file of the application belongs.

If your selection in the **Add by criterion** drop-down list is **Metadata**, set the check boxes opposite executable file properties that you want to use in the condition that triggers the rule: **File name**, **File version**, **Application name**, **Application version**, **Vendor**.

- e. Set 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 have been started on the virtual machine, 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 more conditions that trigger the rule: **Metadata**, **Folder path**, **File hash code (MD5)**, or **KL category** to which the executable file of the application belongs.

If your selection in the **Add by criterion** drop-down list is **Metadata**, set the check boxes opposite executable file properties that you want to use in the condition that triggers the rule: **File name**, **File version**, **Application name**, **Application version**, **Vendor**.
 - b. Set 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 **"KL category" condition(s)**. 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 **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 based on storage device**. To do so:
 - a. In the **Condition based on storage device** 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 (see page [25](#)).
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 list of rules, select the rule whose status you want to edit.
4. In the **Status** column, left-click to bring up the context menu of the column, and select the appropriate rule status:
 - 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 you attempt to start an application that is blocked by an Application Startup Control rule, Kaspersky Security displays a message that the application is blocked from starting. If you believe that the application is blocked from starting by mistake, you 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 (see page [25](#)).
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 **Message 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 **Blocking** 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 **Default** and **Variables** buttons.
6. Click **OK**.
7. To save changes, click the **Save** button.

Application Privilege Control

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system and you selected "Standard installation" as the type of installation.

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

In this section:

About Application Privilege Control	138
Enabling and disabling Application Privilege Control	139
Placing applications into groups	141
Moving an application to a trusted group	143
Working with application control rules	144
Protecting operating system resources and personal data	151

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 personal data.

This component controls the activity of applications on the protected virtual machine, 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 resources of the protected virtual machine.

Network activity of applications is monitored by the Firewall component (see section "About Firewall" on page [79](#)).

When an application is started on the protected virtual machine for the first time, Application Privilege Control scans the application and places it in one of the *trust groups*. A trust group defines the application control rules that Kaspersky Security applies when controlling application activity.

We recommend that you participate in Kaspersky Security Network to improve the performance of Application Privilege Control (see *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). 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.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
- From the application settings window (see section "Application settings window" on page [25](#)).


► *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. Open the **Endpoint control** section.
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.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *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 Application Privilege Control component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 on the protected virtual machine for the first time, Application Privilege Control scans the application and places it in one of the trust groups.

At the first stage of the application scan, Kaspersky Security searches the internal database of known applications for a matching entry and then sends a request to the Kaspersky Security Network database (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 Internet Security uses the heuristic analysis to assign unknown applications (those not included in the Kaspersky Security Network database and lacking the signature of a trusted vendor) to trust groups. During heuristic analysis, Kaspersky Security identifies the threat level of an application. Kaspersky 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 Security automatically assigns all unknown applications.

By default, Kaspersky Security scans an application for 30 seconds. If the threat level of the application has not been determined after this time, Kaspersky Security assigns the application to the Low Restricted group and continues its attempt to determine the threat level

of the application in background mode. After completing this process, Kaspersky 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 protected virtual machine do not pose a threat to security, you can reduce the amount of time that is allocated for determining the threat level of applications. If you install applications whose safety is questionable on the protected virtual machine, you are advised to increase the amount of time that is allocated for determining the threat level of applications.

If an application has a high threat level, Kaspersky Security notifies the user, prompting you 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 the virtual machine, 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 (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. If you want to automatically place digitally signed applications in the Trusted group, select the **Trust applications that have a digital signature** check box.
4. Choose the way in which unknown applications are to be assigned to trust groups:
 - To use heuristic analysis for assigning unknown applications to trust groups, select **Use heuristic analysis to assign group** and specify the amount of time allocated for scanning the application that is launched in the **Maximum time to assign group** field.
 - 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. To save changes, click the **Save** button.

Moving an application to a trusted group

When an application is first started, Kaspersky 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, you are advised to edit the rules for an individual application (see section "Editing an application control rule" on page [146](#)).

► *To move an application to a trust group:*

1. Open the application settings window (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Click the **Applications** button.

The **Applications** window opens.

4. Select the **Application control rules** tab.
5. In the list of applications, select the desired application.
6. Do one of the following:

- Right-click to display the context menu of the application. In the context menu of the application, select **Move to → group <group name>**.
- Open the context menu by clicking the **Trusted / Low Restriction / High Restriction / Untrusted** link in the bottom left corner of the **Application control rules** tab.
In the context menu, select the required trust group.

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

Working with application control rules

By default, application activity is controlled by application control rules that are defined for the trust group to which Kaspersky 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	144
Editing an application control rule.....	146
Disabling downloads and updates of application control rules from the Kaspersky Security Network database	147
Disabling the inheritance of restrictions from the parent process.....	148
Excluding specific application actions from application control rules	150
Configuring storage settings for control rules that govern unused applications.....	151

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 (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Click the **Applications** button.

The **Applications** window opens.

4. Select the **Application control rules** tab.
5. In the list of applications, select the desired trust group or application group.
6. Right-click to bring up the context menu of the trust group or application group and select the **Group rules** item.

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

7. 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. In the **Application group control rules** window, 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 (see page [25](#)).

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 Application Privilege Control component's settings are displayed.

3. Click the **Applications** button.

The **Applications** window opens.

4. Select the **Application control rules** tab.

5. In the list of applications, select the desired application.

6. Do one of the following:

- Right-click to bring up the application's context menu and select **Application rules**.
- Click the **Additional** button in the lower-right corner of the **Application control rules** tab.

The **Application control rules** window opens.

7. 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.
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.**
10. In the **Application control rules** window, click **OK**.
11. In the **Applications** window, click **OK**.
12. To save changes, click the **Save** button.

Disabling downloads and updates of 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 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 (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Clear the **Update control rules for previously unknown applications from KSN databases** 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 section "Editing application control rules" on page [146](#)) 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 (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Click the **Applications** button.

The **Applications** window opens.

4. Select the **Application control rules** tab.
5. In the list of applications, select the desired application.
6. Right-click to bring up the application's context menu and select **Application rules**.

The **Application control rules** window opens.

7. Select the **Exclusions** tab.
8. Select the **Do not inherit restrictions of the parent process (application)** check box.
9. In the **Application control rules** window, 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 (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Click the **Applications** button.

The **Applications** window opens.

4. Select the **Application control rules** tab.
5. In the list of applications, select the desired application.

6. Right-click to bring up the application's context menu and select **Application rules**.

The **Application control rules** window opens.

7. Select the **Exclusions** tab.

8. Select check boxes next to application actions that do not need to be monitored.

- **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.**

9. In the **Application control rules** window, click **OK**.

10. In the **Applications** window, click **OK**.

11. 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 (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Do one of the following:
 - If you want Kaspersky Security to delete control rules of unused applications, select the **Delete rules for applications that are not started 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 rules for applications that are not started for more than** check box.
4. To save changes, click the **Save** button.

Protecting operating system resources and personal data

Application Privilege Control manages application rights to take actions on various categories of operating system resources and of personal 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	152
Adding a protected resource	153
Disabling resource protection	154

Adding a category of protected resources

► *To add a new category of protected resources:*

1. Open the application settings window (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Click the **Resources** button.

The **Applications** window opens.

4. Select the **Protected resources** tab.
5. 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.
6. In the upper-left part of the **Protected resources** tab, click to open the context menu of the **Add** button.

7. In the context menu, select **Category**.

The **Category of protected resources** window opens.

8. Enter the name for the new category of protected resources.

9. Click **OK**.

A new item appears in the list of categories of protected resources.

10. In the **Applications** window, click **OK**.

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

Adding a protected resource

► *To add a protected resource:*

1. Open the application settings window (see page [25](#)).

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 Application Privilege Control component's settings are displayed.

3. Click the **Resources** button.

The **Applications** window opens.

4. Select the **Protected resources** tab.

5. 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.

6. In the upper-left part of the **Protected resources** tab, click to open the context menu of the **Add** button.

7. In the context menu, select the type of resource that you want to add:

- **File or folder.**
- **Registry key.**

The **Protected resource** window opens.

8. In the **Name** field, enter a name for the protected resource.
9. Click the **Browse** button.
10. In the window that opens, specify the necessary settings depending on the type of protected resource that you want to add. Click **OK**.
11. 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.

12. In the **Applications** window, click **OK**.
13. To save changes, click the **Save** button.

Disabling resource protection

► *To disable resource protection:*

1. Open the application settings window (see page [25](#)).
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 Application Privilege Control component's settings are displayed.

3. Click the **Resources** button.

The **Applications** window opens.

4. Select the **Protected resources** tab.

5. 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.

- Add the resource to the list of exclusions from protection by the Application Privilege Control component. To do so:
 - a. Click the **Exclusions** button in the upper right part of the **Protected resources** tab.
 - b. In the **Exclusions** window that opens, left-click to bring up the context menu of the **Add** button.
 - c. 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.

- d. In the **Name** field, enter a name for the protected resource.
- e. Click the **Browse** button.
- f. 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.
- g. Click **OK**.
- h. 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.

- i. In the **Exclusions** window, click **OK**.
6. In the **Applications** window, click **OK**.
 7. To save changes, click the **Save** button.

Device Control

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system and you selected "Standard installation" as the type of installation.

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

In this section:

About Device Control	157
Enabling and disabling Device Control	157
About rules of access to devices and connection buses.....	159
About trusted devices.....	159
Standard decisions on access to devices.....	160
Editing a device access rule	162
Editing a connection bus access rule	163
Actions with trusted devices	164
Editing templates of Device Control messages	167
Obtaining access to a blocked device	168

About Device Control

Device Control ensures the security of confidential data by restricting user access to devices that are installed on the protected virtual machine or connected to it:

- Data storage devices (hard drives, removable drives, CDs/DVDs)
- Network devices (modems, external network cards)
- Printing devices (printers)
- Connection buses (also referred to as "buses"), i.e. interfaces for connecting devices to the protected virtual machine (such as USB or FireWire)

Device Control manages user access to devices by applying *device access rules* (see section "*About rules of access to devices and connection buses*" on page [159](#)) (also referred to as "access rules") and *connection bus access rules* (also referred to as "bus access rules").

By default, access to all types of devices and connection buses is allowed for all users at all times, and the logging of blocked attempts to access devices and connection buses in application reports is enabled.

Enabling and disabling Device Control

By default, Device Control is enabled. You can disable Device Control, if necessary.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "*Main application window*" on page [23](#)).
- From the application settings window (see section "*Application settings window*" on page [25](#)).

► *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. Open the **Endpoint control** section.
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.
 - To disable Device Control, select **Disable** in the menu.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable Device 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 **Device Control**.

In the right part of the window, the Device Control component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 rules of access to devices and connection buses

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.

The connection bus access rule allows or blocks access to the 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 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.

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 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 Security makes a decision on whether to allow access to a device after you connect the device to the protected virtual machine.

Table 2. Standard decisions on access to devices

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	
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.
The device is trusted.	Included in the list of trusted devices.	Not subject to scanning.	Not subject to scanning.	Access allowed.
Access to the device is allowed.	Not included in the list of trusted devices.	Access allowed.	Not subject to scanning.	Access allowed.
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.

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	
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.
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.
Access to the device is blocked.	Not included in the list of trusted devices.	Access blocked.	Not subject to scanning.	Access blocked.
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.
There is no device access rule.	Not included in the list of trusted devices.	No access rule.	Access allowed.	Access allowed.
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 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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the Device Control component's settings are displayed.

3. 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 **Configuring device access rules** 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 overall 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, set 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 so, in the **Rights of the selected group of users by access schedules** table, set the check boxes in the columns with the names of the relevant operations.
- f. Repeat steps c–e for the remaining items in the **Users and / or groups of users** list.
- g. Click **OK**.

Editing the default settings of device access rules causes the setting of access to the device type to change to *Restrict by rules*.

7. If necessary, edit the values of the access parameter on the **Device types** tab in the Device Control settings window:
 - To allow access to a type of devices, left-click the **Access** column to bring up a context menu and select **Allow**.
 - To block access to a type of devices, left-click the **Access** column to bring up a context menu and select **Block**.
8. 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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the Device Control component's settings 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

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.

In this section:

Adding a device to the list of trusted devices.....	164
Editing the Users setting of a trusted device.....	166
Removing a device from the list of trusted devices.....	166

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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the Device Control component's settings are displayed.

3. Select the **Trusted devices** tab.
4. Click the **Select** button.

The **Select trusted devices** window opens.

5. Set 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.

6. Click the **Select** button.

The **Select Users or Groups** window in Microsoft Windows opens.

7. Specify users and / or groups for whom Kaspersky Security should recognize 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.

8. In the **Select 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.

9. Repeat steps 4-8 for each device that you want to add to the list of trusted devices for the specified users and / or user groups.

10. 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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the Device Control component's settings are displayed.

3. Select the **Trusted devices** tab.
4. In the list of trusted devices, select a device whose settings you want to edit.
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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the Device Control component's settings 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 Security based on device access rules and connection bus access rules.

Editing templates of Device Control messages

When you attempt to access a blocked device, Kaspersky Security displays a message that access to the device is blocked or that the operation with the device content is forbidden. If you believe that access to the device is blocked (or that an operation with device content is forbidden) by mistake, you 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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Device Control**.

In the right part of the window, the Device Control component's settings are displayed.

3. In the right part of the window, click the **Templates** button.

The **Message 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 **Blocking** 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 **Default** and **Variables** buttons.
6. Click **OK**.
7. To save changes, click the **Save** button.

Obtaining access to a blocked device

You can gain 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 Security functionality that grants temporary access to a device is available only when Kaspersky Security operates under the Kaspersky Security Center policy and this functionality is enabled in the policy settings (see *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*).

► *To obtain access to a blocked device from the Device Control component settings window:*

1. Open the main application window (see page [23](#)).
2. Select the **Protection and Control** tab.
3. Open the **Endpoint control** section.
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. Select **Access to device** in the menu.

The **Request access to device** window opens.

6. From the list of connected devices, select a device to which you want to gain access.

7. Click the **Get access code** button.

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

8. In the **Access duration** field, specify the time interval for which you want to have access to the device.
9. Click the **Save** button.

The standard **Save access key** window of Microsoft Windows opens.

10. Select the folder in which you want to save a file with a device access key, and click the **Save** button.

11. Pass the device access key file to the LAN administrator.

12. Receive the device access code from the LAN administrator.

13. In the **Request access to device** window, click the **Activate access code** button.

The standard **Open access key** window in Microsoft Windows opens.

14. Select the device access key file that was received from the LAN administrator, and click the **Open** button.

The **Activating the access code for the device** window opens and displays information about the provided access.

15. In the **Activating the access code for the device** 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. 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. Select the device access key file that was received from the LAN administrator, and click the **Open** button.

The **Activating the access code for the device** window opens and displays information about the provided access.

9. In the **Activating the access code for the device** 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.

Web Control

This component is available if Kaspersky Security is installed on a virtual machine with a Windows desktop operating system and you selected "Standard installation" as the type of installation.

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

In this section:

About Web Control.....	171
Enabling and disabling Web Control.....	172
About web resource access rules.....	174
Actions with web resource access rules	175
About Web Control messages.....	187
Editing templates of Web Control messages	187

About Web Control

Web Control monitors user activity on the corporate LAN, making it possible to limit or block 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 features:

- 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 "News media" category). For a more detailed description of content categories, see the Knowledge Base (<http://support.kaspersky.com/13175>).

- 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 section "About web resource access rules" on page [174](#)).

Enabling and disabling Web Control

By default, Web Control is enabled. You can disable Web Control, if necessary.

You can enable or disable a component in two ways:

- On the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).
- From the application settings window (see section "Application settings window" on page [25](#)).

► *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. Open the **Endpoint control** section.
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 **Enable** in the menu.
 - To disable Web Control, select **Disable** in the menu.

If this menu item is unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

► *To enable or disable Web 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 **Web Control**.

In the right part of the window, the Web Control component's settings are displayed.

If component settings are unavailable, this means that you cannot enable or disable this component because the policy-defined setting is applied to protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 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 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 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 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 Security monitors access to web resources covered by the rule.

After Kaspersky Security has been installed, the Web Control component has two preset rules:

- The **Scripts and stylesheets** 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.
- Export or import the list of web resource addresses of the rule.

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.

- Edit a rule.
- Edit rule priority.

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 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.

- 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	176
Rules for creating masks for web resource addresses	179
Exporting and importing the list of web resource addresses.....	182
Testing web resource access rules	184
Changing the priority web resource access rules	185
Enabling and disabling a web resource access rule	186

Adding and editing a web resource access rule

► *To add or edit a web resource access rule:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the Web Control component's settings are displayed.

3. Do one of the following:
 - To add a rule, click the **Add** button.
 - If you want to edit a rule, select it in the list of rules and click the **Edit** button.

The **Web resource access 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. 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. Set the check boxes next to the names of the required content categories and / or data type categories.

Setting the check box next to the name of a content category and / or data type category means that Kaspersky 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. To create a list of web resources addresses, you can use a *web resource address mask* (hereinafter also "address mask") (see section "Rules for creating masks for web resource addresses" on page [179](#)).

After creating a list of web resource addresses, you can export this list to file in order to be able to import this list from file subsequently (see section "Exporting and importing the list of web resource addresses" on page [182](#)).

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 Security allows access to web resources that match the parameters of the rule.

- **Block.** If this value is selected, Kaspersky Security blocks access to web resources that match the parameters of the rule.
 - **Warn.** If this value is selected, Kaspersky Security displays a message to warn that a web resource is unwanted when the user attempts to access web resources that match the parameters of the rule. By using links from the warning message, the user can obtain access to the requested web resource.
- 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 **Web resource access rule** window, click **OK**.
6. To save changes, click the **Save** button.

Rules for creating masks for web resource addresses

Using a web resource 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 resource addresses 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. A sequence of *. characters at the beginning of an address mask is interpreted as *. or an empty string.

Example: the address mask `http://www*.example.com` covers the address of the web resource `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 of web resources with any network protocol.

Example: the address mask http://example.com covers the web resource addresses https://example.com.
 - If the address mask contains a network protocol, this address mask only covers web resource addresses with the same network protocol as that of the address mask.

Example: the address mask http://*.example.com covers the web resource address http://www.example.com but does not include 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.

No.	Address mask	Address of web resource to verify	Is the address covered by the address mask	Comment
4	*example.com	http://www.123.example.com	Yes	See rule 1.
5	http://www.*.example.com	http://www.123example.com	No	See rule 1.
6	www.example.com	http://www.example.com	Yes	See rules 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.

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 (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.
In the right part of the window, the Web Control component's settings 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 **Web resource access rule** window opens.

A list of web resource addresses to which the rule applies appears under the **Apply to addresses** drop-down list.

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.

8. Select the file to which you want to export the list of web resource addresses, and click the **Save** button.

► *To import the list of web resource addresses from a file into a rule:*

1. Open the application settings window.
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the Web Control component's settings are displayed.

3. Do one of the following:
 - To create a new rule, click the **Add** button.
 - If you want to edit a rule, select it in the list of rules and click the **Edit** button.

The **Web resource access rule** window opens.

4. 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.

5. 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.

6. 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 standard **Open file** window in Microsoft Windows opens.

7. In the **Open file** window in Microsoft Windows, select a file with a list of web resource addresses to import.
8. Click the **Open** button.
9. In the **Web resource access rule** window, click **OK**.
10. To save changes, click the **Save** button.

Testing web resource access rules

You can test web resource access rules. To do so, the Web Control component includes Rules diagnostics. A completed rule test is followed by a message with information about the action that is taken by Kaspersky Security, according to the first rule that is triggered on the attempt to access the specified web resource(s) (allow, block, or warn). All triggered rules are tested next.

► *To test the web resource access rules:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the Web Control component's settings 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 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 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. To do so:
 1. 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.

2. In the **Select Users or Groups** window in Microsoft Windows, specify the relevant users and / or user groups and click **OK**.
 - c. If you want to test the rules that Kaspersky 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**), and select check boxes opposite the names of the relevant content categories and / or categories of data types.
 - 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. Specify the day of the week and time on the right.
5. Click the **Validate** button.

Test completion is followed by a message on the right of the **Validate** button with information about the action that is taken by Kaspersky Security, according to the first rule that is triggered on the attempt to access the specified web resource(s). 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 table in the lower part of the **Rules diagnostics** window lists the remaining triggered rules, specifying the action taken by Kaspersky Security. The rules are listed in the order of declining priority.

Changing the priority web resource access rules

You can change the priority to each web resource access rule from the list of rules by arranging the rules in a certain order.

You cannot change the priority of the "Default rule". It always has the lowest priority and is located at the end of the list of rules.

► *To change the priority of web resource access rules:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the Web Control component's settings are displayed.
3. In the list of rules, 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.

Enabling and disabling a web resource access rule

► *To enable or disable a web resource access rule:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the Web Control component's settings are displayed.
3. In list of rules, 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.

About Web Control messages

Depending on the type of action that is specified in the properties of web resource access rules, Kaspersky Security displays a message of one of the following types when you attempt to access Internet resources (the application substitutes an HTML page with a message for the HTTP server response):

- **Warning message.** This message warns the user that a website is unwanted and / or does not comply with the corporate policy. Kaspersky 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 website.

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 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 (see section "Editing templates of Web Control messages" on page [187](#)).

Editing templates of Web Control messages

► *To change the template for Web Control messages:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Endpoint control** section, select **Web Control**.

In the right part of the window, the Web Control component's settings are displayed.

3. In the right part of the window, click the **Templates** button.

The **Message 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 website 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 website is blocked, select the **Blocking** 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 **Default** and **Variables** buttons.

6. Click **OK**.

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

Scanning the virtual machine

This section describes the specifics and settings of scan tasks, security levels, scan methods and technologies, and instructions on handling files that Kaspersky Security has not processed when scanning the virtual machine for viruses and other threats.

In this section:

About scan tasks.....	189
Starting or stopping a scan task	190
Configuring scan task settings.....	191
Handling unprocessed files	207

About scan tasks

A virus scan is vital to virtual machine security. You are urged to regularly scan the virtual machine 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.

To find viruses and other malware, Kaspersky Security includes the following scan tasks:

- **Full Scan.** A thorough scan of the guest operating system installed on the protected virtual machine. By default, Kaspersky Security scans the following objects:
 - System memory
 - Objects that are loaded at startup of the operating system
 - Operating system backup
 - All hard drives and removable drives connected to the protected virtual machine
- **Critical Areas Scan.** By default, Kaspersky Security scans objects that are loaded at operating system startup.

- **Custom Scan.** Kaspersky Security scans objects 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 drives, removable drives, and network drives connected to the protected virtual machine
 - 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 scan scope.

After scan tasks start, their completion progress is displayed in the field next to the name of the running scan task, in the **Tasks** section on the **Protection and Control** tab of the main application window (see section "Main application window" on page [23](#)).

Information on the scan results and events that have occurred during the performance of scan tasks is logged in a Kaspersky Security report.

Starting or stopping a scan task

Regardless of the selected scan task run mode, (see section "Selecting the scan task run mode" on page [203](#)), you can start or stop a scan task at any time.

► *To start or stop a scan task:*

1. Open the main application window (see page [23](#)).
2. Select the **Protection and Control** tab.
3. Open the **Tasks** section.

4. Click the row with the name of a scan task.

A menu with scan task actions opens.

If some of the scan tasks do not appear in the section, this means that the policy prohibits management of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 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 name of this scan task changes to *Stopped*.

You can also start a custom scan of any file by calling up the Windows context menu and selecting the **Scan for viruses** item.

Configuring scan task settings

To configure scan task settings, you can perform the following:

- Change the security level.

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

- Change the action that is performed by Kaspersky Security on detection of 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 the scanning of files: shorten the scan duration and speed up Kaspersky 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 Security excludes the file from the current scan (except archives and objects that include several files).

- Configure scanning of compound files.
- Configure Heuristic Analyzer.

When active, Kaspersky Security uses signature analysis. During signature analysis, Kaspersky Security matches the detected object with records in the application 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, Kaspersky 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 application database.

- Configure the use of iSwift scanning technology.

You can enable the use of the iSwift technology, which optimizes the speed of file scanning by excluding files that have not been modified since the most recent scan. iSwift technology also involves using SharedCache technology that optimizes the speed of file scanning by excluding files that have been already checked on a different virtual machine from scanning.

- Select the scan task run mode.

If it is impossible to run the scan task for any reason (for example, the protected virtual machine 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 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 Security.

- Configure the scan task to run under a different user account.
- Specify the settings for scanning removable drives when they are connected to the protected virtual machine.

In this section:

Changing the security level	193
Changing the action to take on infected files	194
Editing the scan scope	195
Optimizing file scanning	199
Scanning compound files	200
Configuring Heuristic Analyzer	201
Configuring the usage of iSwift technology.....	202
Selecting the scan task run mode	203
Starting a scan task under the account of a different user	205
Scanning removable drives when they are connected to the virtual machine	206

Changing the security level

To perform scan tasks, Kaspersky Security uses various combinations of settings. These groups of settings are called *security levels*. There are three security levels: **High**, **Recommended**, and **Low**. The **Recommended** security level is considered the optimal setting, and is recommended by Kaspersky Lab.

► To change a security level:

1. Open the application settings window (see page [25](#)).
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.**
- **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. In the **Security level** section, do one of the following:

- To apply one of the preset security levels (**High, Recommended, Low**), select it with the slider.
- If you want to configure a custom 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 security level, the name of the security level in the **Security level** section changes to **Custom**.

- To change the 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 (see page [25](#)).
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.**
 - **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. In the **Action on threat detection** section, select the required option:

- **Select action automatically.**

This option is selected by default. On detecting a threat the application performs the action **Disinfect. Delete if disinfection fails.**

- **Perform action: Disinfect. Delete if disinfection fails.**
- **Perform action: Disinfect.**

Regardless of the option selected, Kaspersky Security applies the **Delete** action to files that are part of the Windows Store application.

- **Perform action: Delete.**
- **Perform action: Inform.**

When they are deleted or disinfected, copies of files are saved in Backup.

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 the application scans when performing a scan task.

To create the scan scope:

- Create lists of objects to be scanned by Kaspersky Security.
- Select a type of files to be scanned.

► *To create the scan scope:*

1. Open the main application window (see page [23](#)).
2. Select the **Protection and Control** tab.
3. Open the **Tasks** section.
4. Click a row with the name of the scan task that you need:
 - **Full Scan.**
 - **Critical Areas Scan.**
 - **Custom Scan.**

A menu with scan task actions opens.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

5. Select the **Scan scope** menu item.

The **Scan scope** window opens.

6. In the **Scan scope** window, do one of the following:

- To add a new object to the list of objects to be scanned, click the **Add** button.

The **Select object** window opens.

- If you want to change the path to an object, select one from the list of objects and click the **Edit** button.

The **Select object** window opens.

- If you want to remove an object from the scan scope, select one from the list of objects and click the **Delete** button.

A window for confirming deletion opens.

You cannot remove or edit objects that are included in the default scan scope.

7. In the **Select object** window, do one of the following:

- If you want to add a new object, select one in the **Select object** window and click the **Add** button.

All objects that are selected in the **Select object** window are displayed in the list of objects in the **Scan scope** window.

Click **OK**.

- To change the path to an object in the list of objects, enter a different path to the object in the **Object** field and click **OK**.
- If you want to remove an object, click the **Yes** button in the window for confirming removal.

8. If necessary, repeat steps 6 and 7 to add objects, change the path to objects, or remove objects from the scan scope.

9. If you want to exclude an object from the scan scope, clear the check box next to the object in the **Scan scope** list. The object remains on the list of objects to be scanned, but it is not scanned when the scan task runs.

10. In the **Scan scope** window, click **OK**.

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

► *To select the type of scanned objects:*

1. Open the application settings window.

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.**
- **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 can send a virus or other malware to your virtual machine in an executable file that has had its extension changed to .txt. 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, Kaspersky Security 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. Click **OK**.
7. To save changes, click the **Save** button.

Optimizing file scanning

► *To optimize file scanning:*

1. Open the application settings window (see page [25](#)).
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.**
- **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 files that are scanned for longer than** check box and specify the scan duration 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 (see page [25](#)).
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.**
 - **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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

A window with the name of the selected scan task opens.

4. In this window on the **Scope** tab, in the **Scan of compound files** section, specify which compound files you want to scan: archives, installation packages, embedded OLE objects, mail format files or password protected archives, by selecting the corresponding check boxes.
5. 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 set, only new files are scanned.

6. Click the **Additional** button.

The **Compound files** window opens.

7. In the **Size limit** section, do one of the following:

- If you do not want the application 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 the application 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 Security scans large files that are extracted from archives, regardless of whether the **Do not unpack large compound files** check box is set.

8. In the **Compound files** window, click **OK**.

9. In the window with the scan task name, click **OK**.

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

Configuring Heuristic Analyzer

► *To configure the use of heuristic analysis:*

1. Open the application settings window (see page [25](#)).
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.**
 - **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 methods** section:

- If you want the application to use heuristic analysis during the scan task, set the **Heuristic Analysis** check box and use the slider to set the level of heuristic analysis: **light scan**, **medium scan**, or **deep scan**.
- If you do not want the application to use heuristic analysis during the scan task, clear the **Heuristic Analysis** check box.

6. Click **OK**.

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

Configuring the usage of iSwift technology

► *To configure the usage of iSwift technology:*

1. Open the application settings window (see page [25](#)).
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**.
 - **Custom Scan**.

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 **Scanning technology** section, do one of the following:
 - Select the **iSwift technology** check box to use this technology during the scan.
 - Clear the **iSwift technology** check box not to use this technology during the scan.

Enabling the iSwift technology also enables the SharedCache technology.

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 (see page [25](#)).
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.**
 - **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. Click the **Run mode** button.

The **Run mode** tab opens in the window with the name of the selected task.

4. 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**.

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 settings of the scan task run schedule. To do so:
 - a. 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**.
 - b. 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.
 - c. If you want Kaspersky 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.

- d. If you want Kaspersky Security to suspend scan tasks when virtual machine resources are limited, select the **Suspend scheduled scanning when the screensaver is off and the protected virtual machine is unlocked** check box. This run schedule option for the scan task helps to conserve virtual machine resources.

6. Click **OK**.

7. 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 you are logged in to the guest operating system of the protected virtual machine. 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:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select the subsection with the name of the required task:
 - **Full Scan.**
 - **Critical Areas Scan.**
 - **Custom Scan.**

In the right part of the window, the settings of the selected scan task are displayed.

If some of the scan tasks do not appear in the section, this means that the policy prohibits configuring the settings of these scan tasks for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. Click the **Run mode** button.

The **Run mode** tab opens in the window with the name of the selected scan task.

4. In the **User** section, select the **Run task as** check box.
5. In the **Name** field, enter the account name 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 virtual machine

Malware that exploits operating system vulnerabilities to replicate via networks and removable drives has become increasingly widespread lately. Kaspersky Security allows you to scan removable drives that are connected to the virtual machine for viruses and other malware.

- *To configure scanning of removable drives when they are connected to the virtual machine:*

1. Open the application settings window (see page [25](#)).
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 **Action on removable drive connection** dropdown list, select the required action:
 - **Do not scan.**
 - **Full Scan.**
 - **Quick Scan**

If the section is unavailable, this means that the policy prohibits configuring the removable drive scan settings for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

4. If you want Kaspersky Security to scan removable drives of a size less or equal to a specified value, select the **Maximum removable 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 Security has not processed while scanning the virtual machine for viruses and other threats.

In this section:

About unprocessed files	207
Managing the list of unprocessed files.....	208

About unprocessed files

Kaspersky Security logs information about unprocessed files in which it detects a threat. This information is recorded in the form of events in the list of unprocessed files.

An infected file is considered *processed* if Kaspersky Security performs one of the following actions on the infected file according to the specified application settings while scanning the virtual machine for viruses and other malware:

- Disinfect.
- Delete.
- Delete if disinfection fails.

An infected file is considered *unprocessed* if Kaspersky Security for any reason fails to perform an action on the infected file according to the specified application settings while scanning the virtual machine for viruses and other malware.

This situation is possible in the following cases:

- The scanned file is unavailable (for example, it is located on a network drive or on an external device 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 application databases. 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 section "*Deleting files from the list of unprocessed files*" on page [211](#)).
- restore infected files that contain important information and restore files that are marked as *Disinfected* or *Not infected* (see section "*Restoring files from the list of unprocessed files*" on page [210](#)).

Managing the list of unprocessed files

The list of unprocessed files appears in the form of a table.

You can perform the following file operations while managing the list of unprocessed files:

- View the list of unprocessed files.
- Scan unprocessed files using the current version of the application databases.
- 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 the list of unprocessed files by column values or by custom filter conditions.
- Use the unprocessed file search function.
- Sort unprocessed files.
- Change the order and set of columns that are displayed in the list of unprocessed files.
- Group unprocessed files.
- Copy selected entries about unprocessed files to clipboard.

In this section:

Starting a Custom Scan task for unprocessed files	209
Restoring files from the list of unprocessed files.....	210
Deleting files from the list of unprocessed files.....	211

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 Security to scan files after another update of application databases.

► *To start a Custom Scan task for unprocessed files:*

1. Open the main application window (see page [23](#)).
2. In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.
3. Select the **Unprocessed files** tab.

4. In the table on the **Unprocessed files** tab, select one or more files that you want to scan. To select multiple files, select 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 (see page [23](#)).
2. In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.
3. Select the **Unprocessed files** tab.
4. To restore all files:
 - a. Right-click anywhere in the table on the **Unprocessed files** tab to display the context menu.
 - b. Select **Restore all**.

Kaspersky Security moves all the files from the list of the 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 saving the file.

5. To restore one or more files:
 - a. In the table on the **Unprocessed files** tab, select one or more unprocessed files that you want to restore. To select multiple files, 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 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 saving 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 Security creates a backup copy of the file and saves it in Backup in case you need to later restore the file (see section "Restoring files from Backup" on page [232](#)).

► *To delete files from the list of unprocessed files:*

1. Open the main application window (see page [23](#)).
2. In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.
3. Select the **Unprocessed files** tab.
4. In the table on the **Unprocessed files** tab, select one or more files that you want to delete. To select multiple files, 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 Security creates a backup copy of each file and saves the copy in Backup (see section "About Quarantine and Backup" on page [228](#)). Kaspersky Security then deletes the selected files from the list of unprocessed files.

Updating databases and application 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	212
Starting and stopping an update task	213
Selecting the update task run mode	214

About database and application module updates

Updates of application databases keep the protection of your virtual machine up to date. New viruses and other types of malware appear worldwide on a daily basis. Kaspersky Security databases contain information about threats and ways of neutralizing them. The application databases are constantly supplemented with records of new threats. Protection components use this information when searching for and neutralizing infected files on the protected virtual machine. To enable Kaspersky Security to detect new threats in a timely manner, you need to update the databases and application modules regularly.

Database and application module updates can change certain Kaspersky Security settings, for example, heuristic analysis parameters that improve protection and scanning effectiveness.

Kaspersky Security regularly checks a folder on the SVM to which the protected virtual machine is connected for update packages (for details see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). If an update package is available, the application installs an update of the required databases and application modules on the protected virtual machine.

Application database and module updates require a current license to use the application.

An update of databases and application modules is performed by an update task. An update task is started automatically. If necessary, you can start the update task manually (see the section "Starting and stopping an update task" on page [213](#)) or set up a schedule to run the update task.

If application databases and modules have not been updated for a long time, a corresponding message appears in the **Task management** section of the **Protection and Control** tab in the main application window (see section "Main application window" on page [23](#)).

If it is not possible to run the update task for any reason (for example, the virtual machine is off at that time), you can configure the skipped task to be start automatically as soon as this becomes possible.

You can postpone starting the update task after the application starts if you have configured the update task to be run by schedule, and if the start time of Kaspersky 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 Security.

Information on the update results and events that have occurred during the performance of update tasks is logged in a Kaspersky Security report.

Starting and stopping an update task

Regardless of the selected update task run mode, you can start or stop a Kaspersky Security update task at any time.

► *To start or stop an update task:*

1. Open the main application window (see page [23](#)).
2. Select the **Protection and Control** tab.
3. Open the **Tasks** section.
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.

If update tasks do not appear in the section, this means that the policy prohibits configuring the settings of application database and module updates for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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 name of the **Update** task, 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 name of the **Update** task, changes to *Stopped*.

After the update task starts, its completion progress is displayed in the field next to the name of the **Update** task in the **Tasks** section, on the **Protection and Control** tab of the main application window.

Selecting the update task run mode

► *To select the update task run mode:*

1. Open the application settings window (see page [25](#)).
2. In the left part of the window, in the **Scheduled tasks** section, select **Update**.

In the right part of the window, application database update settings are displayed.

If **Update** does not appear in the section, this means that the policy prohibits configuring the settings of application database and module updates for all protected virtual machines in the administration group (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

3. Click the **Run mode** button.

The **Update** window opens.

4. In the **Run mode** section, select one of the following options for starting an update task:

- Select **Automatically** if you want Kaspersky Security to start the update task depending on the availability of the update package on the SVM to which the protected virtual machine is connected (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). The frequency with which the application checks for update packages increases during virus outbreaks and decreases when there are none.

If there are no new updates on the SVM, the update task is not started.

- 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.

When configuring the frequency of the update task, you are advised to take account of the frequency of application database updates on the SVM to which the protected virtual machine is connected (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

- c. In the **Postpone running after application startup for** field, specify the time interval by which the start of the update task is postponed after the startup of Kaspersky Security.

If the **After application startup** item is selected from the **Frequency** drop-down list, the **Postpone running after application startup for** field is not available.

- d. If you want Kaspersky 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.

Trusted zone

This section contains information on the trusted zone and instructions on configuring scan exclusion and creating a list of trusted applications.

In this section:

About the trusted zone	217
Configuring the trusted zone	219

About the trusted zone

A *trusted zone* is a custom list of objects and applications that Kaspersky Security does not monitor when active. In other words, the trusted zone is a set of scan and protection exclusions.

You form the trusted zone on your own, taking into account the features of the objects that are handled and the applications that are installed in the guest operating system of the protected virtual machine. It may be necessary to include objects and applications in the trusted zone when Kaspersky 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;
- folders;
- applications;
- application processes;
- objects according to the classification of Kaspersky Lab's Virus Encyclopedia.

Scan and protection exclusions

Exclusion is a combination of conditions that describe an object or application. If the object satisfies these conditions, Kaspersky Security does not scan this object for viruses or other threats.

Some legitimate applications can be used by criminals to compromise your virtual machine or personal 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. Such applications are not categorized as viruses. Information about legal software that can be used by criminals to harm the computer or personal data is available on the website of the Kaspersky Lab Virus Encyclopedia at <https://securelist.com/threats/riskware/>.

Such applications may be blocked by Kaspersky Security. To prevent them from being blocked, you can configure Kaspersky Security scan and protection exclusions. To do so, add the name or name mask 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. To prevent this application from being blocked, create an exclusion with the name or name mask that is listed in the Kaspersky Lab Virus Encyclopedia.

Exclusions can be used by the following application components and tasks:

- File Anti-Virus.
- Mail Anti-Virus.
- Web Anti-Virus.
- System Watcher.
- Application Privilege Control.
- Scan tasks.

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 Security. By default, Kaspersky 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 Security excludes applications in the list of trusted applications from scanning (see section "Editing the list of trusted applications" on page [225](#)).

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 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 lets you avoid compatibility conflicts between Kaspersky Security applications and other programs (for example, the problem of double-scanning of the network traffic of a third-party computer by Kaspersky Security and by another anti-virus application), and also increases the virtual machine'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. To fully exclude an application from Kaspersky Security scanning and protection, create the exclusion for this application.

If an application that collects information and sends it to be processed is installed on your virtual machine, Kaspersky Security may classify this application as malware. To avoid this, you can exclude the application from scanning by adding it to the list of exclusions.

Configuring the trusted zone

You can configure the trusted zone in the following ways:

- Create a new exclusion.

You can create a new exclusion whereby Kaspersky Security skips the specified files or folders and / or objects with the specified name.

- Suspend an exclusion.

You can temporarily suspend an exclusion without removing it from the list of exclusions.

- Edit the settings of an existing exclusion.

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

- Delete an exclusion.

You can delete an exclusion to stop Kaspersky Security from applying it while protecting and scanning the virtual machine.

- Create a list of trusted applications.

You can create a list of trusted applications for which Kaspersky Security does not monitor file and network activity (including malicious activity) and access to the system registry.

- Suspend the exclusion of a trusted application from Kaspersky Security scanning.

You can temporarily suspend the exclusion of a trusted application from Kaspersky Security application scanning without removing the application from the list of trusted applications.

In this section:

Creating an exclusion.....	221
Editing an exclusion	223
Removing an exclusion	223
Enabling or disabling an exclusion	224
Editing the list of trusted applications	225
Including or excluding a trusted application from scanning.....	227

Creating an exclusion

Kaspersky Security does not scan an excluded object when a hard drive or folder that contains this object is specified at the start of a scan task. However, if you start a custom scan task for an object, Kaspersky Security scans the object even if you have created an exclusion for this object.

► *To create an exclusion:*

1. Open the application settings window (see page [25](#)).

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 zone** section, click the **Settings** button.

The **Trusted zone** window opens on the **Exclusions** tab.

4. Click the **Add** button.

The **Exclusion** window opens.

5. To exclude a file or folder from protecting and scanning:

a. In the **Settings** section, select the **File or folder** check box.

b. Click the **select file or folder** link in the **Exclusion description** section to open the **Name of file or folder** window. In this window, you can specify the file or folder name or the mask of the file or folder name, or select a file or folder in the folder tree.

c. After selecting the object, click **OK** in the **Name of file or folder** window.

A link to the added object appears in the **Exclusion description** section of the **Exclusions** window.

6. To exclude objects with certain names according to the Kaspersky Lab Virus Encyclopedia classification of malicious programs and other threats from protecting and scanning:
 - a. In the **Settings** section, select the **Object name** check box.
 - b. Click the **enter object name** link in the **Exclusion description** section to open the **Object name** window. In this window, you can enter the object name or name mask according to the classification of the Kaspersky Lab Virus Encyclopedia.
 - c. Click **OK** in the **Object name** window.
7. In the **Comment** field, enter a brief description of the exclusion that you are creating.
8. Specify the Kaspersky Security components that should use the exclusion:
 - a. Click the **any** link in the **Exclusion description** section to open the **select components** link.
 - b. Clicking the **select components** link to open the **Protection components** window.
 - c. Select the needed components.
 - d. In the **Protection components** window, click **OK**.

If the components are specified in the settings of the exclusion, the object is not scanned only by these components of Kaspersky Security.

If the components are not specified in the settings of the exclusion, the object is not scanned by all components of Kaspersky Security.

9. Click **OK** in the **Exclusion** window.

The added exclusion appears in the list of exclusions on the **Exclusions** tab of the **Trusted zone** window. The configured settings of this exclusion appear in the **Exclusion description** section.

10. In the **Trusted zone** window, click **OK**.

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

Editing an exclusion

► *To edit an exclusion:*

1. Open the application settings window (see page [25](#)).

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 **Exclusions** tab.

4. Select the exclusion that you need in the list of exclusions.

5. Click the **Edit** button.

The **Exclusion** window opens.

6. Edit the settings of an exclusion.

7. Click **OK** in the **Exclusion** window.

The edited settings of this exclusion appear in the **Exclusion description** section.

8. In the **Trusted zone** window, click **OK**.

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

Removing an exclusion

► *To delete an exclusion:*

1. Open the application settings window (see page [25](#)).

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 **Exclusions** tab.

4. Select the exclusion that you need in the list of exclusions.
5. Click the **Delete** button.

The deleted exclusion disappears from the list of exclusions on the **Exclusions** tab of the **Trusted zone** window.

6. In the **Trusted zone** window, click **OK**.

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

Enabling or disabling an exclusion

► *To enable or disable an exclusion:*

1. Open the application settings window (see page [25](#)).

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 **Exclusions** tab.

4. Select the exclusion that you need in the list of exclusions.

5. Do one of the following:

- Set the check box next to the name of an exclusion if you want to use this exclusion.
- Clear the check box next to the name of this exclusion if you want to suspend this exclusion temporarily.

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 (see page [25](#)).

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. 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 virtual machine, 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** window in Microsoft Windows opens.

c. Select the application that you want to add to the list of trusted applications.

The **Exclusions for application** window opens.

d. 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.**

e. 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 list of trusted applications.
- 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 section "Including or excluding a trusted application from scanning" on page [227](#)). 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 list of trusted applications.
- 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 a trusted application in the scan scope or exclude a trusted application from scanning:*

1. Open the application settings window (see page [25](#)).

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. 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 Security scanning, set the check box next to its name.
- To include a trusted application in Kaspersky Security scanning, clear the check box next to its name.

7. Click **OK**.

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

Backup

This section contains instructions on how to manage Backup.

In this section:

About Backup.....	228
Configuring Backup settings.....	229
Managing Backup	231

About Backup

Backup storage is a list of backup copies of files that have been deleted or modified during the disinfection process. *Backup copy* is a file copy created at the first attempt to disinfect or delete this file. Backup copies of files are stored in a special format and do not pose a threat.

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

When the application is removed, Backup files are removed from the protected virtual machine.

Configuring backup settings

You can configure Backup settings as follows:

- Configure the maximum storage term for backup copies in Backup.

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

- Configure the maximum Backup size.

By default, the maximum Backup size is 100 MB. When data storage reaches its limit, Kaspersky Security automatically deletes the oldest files from Backup so that the maximum data storage size is not exceeded. You can cancel the Backup size limit or change the maximum size.

In this section:

Configuring the maximum storage term for files in Backup	229
Configuring the maximum size of Backup	230

Configuring the maximum storage term for files in Backup

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

1. Open the application settings window (see page [25](#)).
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 **Backup Settings** section, perform one of the following:
 - Set the **Store files no longer than** check box to limit the period during which backup copies of files are stored in Backup. In the field on the right of the check box, specify the maximum storage term for backup copies of files in Backup. The default maximum storage period for backup copies of files in Backup is 30 days.
 - Clear the **Store files no longer than** check box to cancel the limitation on the period during which backup copies of files are stored in Backup.
4. To save changes, click the **Save** button.

Configuring the maximum size of Backup

► *To configure the maximum Backup size:*

1. Open the application settings window (see page [25](#)).
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 Backup, in the **Backup Settings** section in the right part of the window, select the **Maximum storage size** check box. In the field on the right of the check box, specify the maximum size of 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 **Backup Settings** section, clear the **Maximum storage size** check box.

The Backup size limit is disabled by default.

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

Managing Backup

If malicious code is detected in the file, Kaspersky Security blocks the file, removes it from its original folder, places its copy in Backup, and attempts to disinfect the file. 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.

On detecting malicious code in a file that is part of the Windows Store application, Kaspersky Security immediately deletes the file without moving it to Backup. You can restore the integrity of the Windows Store application using tools of the Microsoft Windows operating system.

Kaspersky Security automatically deletes backup copies of files with any status from Backup after the storage term configured in the application settings has elapsed (see section "Configuring the maximum storage term for files in Quarantine and file copies in Backup" on page [229](#)).

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.

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 the list of backup copies of files by column values or by custom filter conditions.
- Use the file backup copy search function.
- Sort backup copies of files.
- Group backup copies of files.
- Change the order and set of columns that are displayed in the list of backup copies of files.
- Copy selected backup copies of files to clipboard.

In this section:

Restoring files from Backup	232
Deleting backup copies of files from Backup	233

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 (see page [23](#)).
2. In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.
3. 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 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 copies of files. To select multiple backup copies, select them while holding down the **CTRL** key.
 - b. Restore files in one of the following ways:
 - Click the **Restore** button.
 - Right-click to bring up the context menu and select **Restore**.

Kaspersky 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 (see page [23](#)).
2. In the upper part of the main application window, click the **Reports** link to open the **Reports and Storages** window.
3. Select the **Backup** tab.
4. To delete all backup copies of files from Backup, do one of the following:
 - Right-click anywhere in the table on the **Backup** tab to display the context menu and select the **Clear storage** item.
 - Click the **Clear storage** button.
5. To delete one or more backup copies of files from Backup:
 - a. In the table, on the **Backup** tab, select one or more backup copies of files. To select multiple backup copies, select them while holding down the **CTRL** key.
 - b. Delete backup copies of files in one of the following ways:
 - Click the **Delete** button.
 - Right-click to display the context menu and select **Delete**.

Managing Reports

This section describes how you can configure report settings and manage reports.

In this section:

Principles of managing reports	234
Configuring report settings	236
Generating reports	238
Viewing reported event information in a separate section.....	238
Saving a report to file	239
Removing information from reports	241

Principles of managing reports

Information about the activity of Kaspersky Security, performance of each scan task and update 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 your interaction with the application and in the course of application operation in general, which are unrelated to any particular Kaspersky Security component or task.
- All protection components report. Contains information about events that are logged in the course of operation of the following Kaspersky 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 Security component or task. Contains information about events that occur in the course of operation of a selected Kaspersky Security component or task.

Event importance levels are of the following types:

-  icon. **Information 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 Security.
-  icon. **Critical events.** Events of critical importance and faults that indicate problems in the operation of Kaspersky Security.

You can manage report data as follows:

- Filter the list of events by column values or by custom filter conditions.
- 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.
- Save the report to a text file.

You can also delete report information on Kaspersky Security components and tasks that are combined into groups. Kaspersky 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 Security is 30 days. After that period of time, Kaspersky 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 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	236
Configuring the maximum size of the report file.....	237

Configuring the maximum report storage term

► *To modify the report maximum storage term:*

1. Open the application settings window (see page [25](#)).
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 parameters** 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 (see page [25](#)).
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 parameters** 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 (see page [23](#)).
2. 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.

3. To generate the All Protection Components report, in the left part of the **Reports and Storages** window in the **Anti-Virus protection** section, 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 Security.

4. 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 relevant 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 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:*

1. Open the main application window (see page [23](#)).
2. 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.

3. 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.

4. If necessary, use the filter, search, and sorting functions to locate the necessary event in the report.
5. 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 generated report to a file in text format (TXT) or a CSV file.

Kaspersky 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:*

1. Open the main application window (see page [23](#)).
2. 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.

3. 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.

4. If necessary, you can modify data presentation in the report by:

- Filtering events
- Running an event search
- Rearranging columns
- Sorting events

5. Click the **Save report** button in the upper right part of the window.

A context menu opens.

6. In the context menu, select the encoding for saving the report file: **Save as ANSI** or **Save as Unicode**.

The standard **Save as** window of Microsoft Office opens.

7. In the **Save as** window, specify the destination folder for the report file.
8. In the **File name** field, type the report file name.
9. In the **File type** field, select the necessary report file format: TXT or CSV.
10. Click the **Save** button.

Removing information from reports

► *To remove information from reports:*

1. Open the application settings window (see page [25](#)).
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 parameters** section, click the **Delete reports** button.

The **Removing information from 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 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 Security components:
 - Application Startup Control.
 - Application Privilege Control.
 - Device Control.
 - Web Control.
- **Data from System Watcher.** Contains information about System Watcher operation.

5. Click **OK**.

Notifications

This section describes notifications alerting the user to events in the operation of Kaspersky Security and provides instructions on configuring event notifications.

In this section:

About Kaspersky Security notifications.....	243
Configuring notifications.....	244

About Kaspersky Security notifications

All sorts of events occur during the operation of Kaspersky 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 Security delivers event notifications in one of the following ways:

- As pop-up notifications in the Microsoft Windows taskbar notification area.
- Via email.

You can configure event notification methods. The notification method is configured for each type of event.

Kaspersky Security supports the logging of information about events in the operation of the application in the event log of Microsoft Windows and / or in Kaspersky Security reports (see page [234](#)).

Configuring notifications

You can configure notifications in the following ways:

- configure logging of Kaspersky Security events (see section "Configuring event logging" on page [244](#));
- configure the display of on-screen notifications (see section "configuring the display of on-screen notifications" on page [245](#));
- configure event notifications via email (see section "Configuring event notifications via email" on page [246](#)).

You can perform the following operations while managing the event table:

- Use the event search function.
- Sort events in ascending or descending order.
- Change the set of columns that are displayed in the list of events.

In this section:

Configuring event logging.....	244
Configuring the display of on-screen notifications.....	245
Configuring event notifications via email	246

Configuring event logging

► *To configure event logging:*

1. Open the application settings window (see page [25](#)).
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 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 logging settings.
6. In columns, set the check boxes next to the required types of events:
 - **Save in application log** if you want to save events in application logs (on page. [234](#)).
 - **Save in Windows event log** if you want to save events in the Microsoft Windows event log.
7. In the **Notifications** window, click **OK**.
8. To save changes, click the **Save** button.

Configuring the display of on-screen notifications

► *To configure the display of on-screen notifications:*

1. Open the application settings window (see page [25](#)).
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 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 on-screen notifications about events.
6. In the **Notify on screen** column, set the check boxes next to the required types of events.

Information about the selected events is displayed on the screen as pop-up notifications in the Microsoft Windows taskbar notification area.

Configuring event notifications via email

► To configure email notifications about events, perform the following steps:

1. Open the application settings window (see page [25](#)).
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 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 event notifications via email.
6. In the **Notify by email** column, set the check boxes next to the required types of events.
7. Click the **Email notification settings** button.

The **Email notification settings** window opens.

8. Select the **Send event notifications** check box to enable the delivery of notifications about Kaspersky Security events selected in the **Notify by email** column.
9. Specify the email notification delivery settings.
10. In the **Email notification settings** window, click **OK**.
11. In the **Notifications** window, click **OK**.
12. To save changes, click the **Save** button.

Performance of Kaspersky Security

This section contains information about the performance of Kaspersky Security and compatibility with other applications, and also guidelines for selecting the types of detectable objects and the operating mode of Kaspersky Security.

In this section:

About Kaspersky Security performance	247
Selecting types of detectable objects	249
Enabling or disabling Advanced Disinfection technology for desktop operating systems	250

About Kaspersky Security performance

The performance of Kaspersky Security means the number of detectable object types and usage of protected virtual machine resources.

Selecting types of detectable objects

Kaspersky Security allows you to flexibly configure the protection of your virtual machine and to select the types of objects (see section "Selecting types of detectable objects" on page [249](#)) that the application detects. Kaspersky Security always scans the operating system for viruses, worms, and Trojans. You cannot disable scanning of these types of objects. Such malware can cause significant harm to the protected virtual machine. For greater security of your virtual machine, you can expand the range of detectable object types by enabling monitoring of legal software that can be used by criminals to damage your virtual machine or personal data.

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 Security performs extensive disinfection that uses a special Advanced Disinfection technology (see section "Enabling or disabling Advanced Disinfection technology for desktop

operating systems" on page [250](#)). *Advanced Disinfection technology* is aimed at purging the operating system of malware that has already started its processes in RAM and that prevents Kaspersky Security from removing it by using other methods. The threat is neutralized when Advanced Disinfection technology is applied. While Advanced Disinfection is in progress, you are advised to refrain from starting new processes or editing the operating system registry. The Advanced Disinfection technology uses considerable operating system resources, which may slow down other applications.

After Advanced Disinfection has been completed on a virtual machine with a Windows desktop operating system, Kaspersky Security requests permission to restart the virtual machine. After virtual machine reboot, Kaspersky Security deletes malware files and starts a "lite" full scan of the virtual machine.

If Kaspersky Security runs on a temporary virtual machine, in case of an active infection of this temporary virtual machine, check a virtual machine template to make sure it is free from viruses and other threats and then restart the temporary virtual machine.

A prompt for a restart of a virtual machine with a Windows server operating system is impossible due to the specifics of Kaspersky Security for server operating systems. An unplanned reboot of a server operating system can lead to problems involving temporary denial of access to server operating system data or loss of unsaved data. It is recommended to reboot a server operating system strictly according to schedule. For this reason, Active Disinfection technology on a protected virtual machine with a Windows server operating system is disabled by default.

If active infection is detected on a protected virtual machine with a Windows server operating system, an event is relayed to Kaspersky Security Center with information that Active Disinfection is required. To disinfect an active infection of a protected virtual machine with a Windows server operating system, enable Active Disinfection technology for server operating systems and start a group task for a virus scan at a time that is convenient for users of the server operating system (see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*).

Selecting types of detectable objects

► *To select types of detectable objects:*

1. Open the application settings window (see page [25](#)).

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 **Objects** section, click the **Settings** button.

The **Objects for detection** window opens.

4. Select check boxes opposite the types of objects that you want Kaspersky Security to detect:

- **Malicious tools.**
- **Adware.**
- **Auto-dialers.**
- **Other.**
- **Packed files.**
- **Multi-packed files.**

Note that any detected objects can be deleted by the application.

5. In the **Objects for detection** window, click **OK**.

The **Objects for detection** window closes. In the **Objects** section, the selected types of objects are listed under **Detection of objects of the following types is enabled**.

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

Enabling or disabling Advanced Disinfection technology for desktop operating systems

► To enable or disable Advanced Disinfection technology for desktop operating systems:

1. Open the application settings window (see page [25](#)).
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.

If the check box is unavailable, this means that you cannot enable or disable Advanced Disinfection technology for desktop operating systems because doing so is prohibited by a policy applied to all protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

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

Kaspersky Security Self-Defense

This section describes the self-defense and remote control defense mechanisms of Kaspersky Security and provides instructions on configuring the settings of these mechanisms.

In this section:

About Kaspersky Security Self-Defense	251
Enabling or disabling Self-Defense	251
Enabling or disabling Remote Control Defense	252
Supporting remote administration applications	253

About Kaspersky Security Self-Defense

Kaspersky Security protects the virtual machine against malicious programs, including malware that attempts to block the operation of Kaspersky Security or even delete it from the protected virtual machine.

The stability of the security system on the virtual machine is ensured by the self-defense and remote control defense mechanisms in Kaspersky 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.

Enabling or disabling Self-Defense

The Kaspersky Security Self-Defense mechanism is enabled by default. You can disable Self-Defense, if necessary.

Disabling Self-Defense reduces the level of virtual machine protection against malware.

► *To enable or disable Self-Defense:*

1. Open the application settings window (see page [25](#)).
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 (see page [25](#)).
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 external management of the system service**.
 - To disable the remote control defense mechanism, clear the **Disable external management of the 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 (see page [25](#)).

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. 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 protected virtual machine, 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 **Select file or folder** window in Microsoft Windows opens.

7. Select an application.

The **Exclusions for application** window opens.

8. Select the **Do not monitor application activity** check box.

9. In the **Exclusions for application** window, click **OK**.

The trusted application that you have added appears in the trusted applications list.

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

Password protection

This section contains information on how to restrict access to Kaspersky Security using a password.

In this section:

About restricting access to the application	254
Enabling and disabling password protection.....	255

About restricting access to the application

Multiple users with different levels of computer literacy can share a single virtual machine. If users have unrestricted access to Kaspersky Security and its settings, the overall virtual machine security level may be reduced.

You can restrict access to Kaspersky Security by setting a password and specifying operations for which the application prompts the user for a password:

- all operations (except notifications of dangerous events);
- configure application settings;
- exit the application;
- disable protection components and stop scan tasks;
- disable control components;
- remove / modify / restore the application.

Enabling and disabling password protection

► *To enable or disable password protection:*

1. Open the application settings window (see page [25](#)).
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 Security with a password:
 - a. In the **Password protection** section, select the **Enable password protection** check box.

If the check box is unavailable, this means that you cannot enable or disable password protection because the policy-defined setting is applied to all protected virtual machines within the administration group (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Contact your system administrator.

- b. In the **Password protection** section, click the **Settings** button.

The **Password protection** window opens.
- c. In the **New user name** field, type the name of the user on whose behalf the application will be accessed.
- d. In the **New password** field type a password for accessing the application.
- e. Confirm the password in the **Confirm password** field.
- f. In the **Password scope** section specify the operations with the application for which the user should enter the password:
 - To restrict access to all operations with the application, select the **All operations (except danger notifications)** option.
 - To specify individual operations, select the **Selected operations** option.

g. If you select the **Selected operations** option, set the check boxes next to the names of the necessary operations:

- **Configure application settings.**
- **Exit the application.**
- **Disable protection components and stop scan tasks.**
- **Disable control components.**
- **Remove / modify / restore the application.**
- **View reports.**

h. Click the **OK** button.

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>).

4. To cancel password restriction of access to Kaspersky 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 the application is removed.
- If the operation of canceling password protection is password-protected, the **Password check** window appears. This window appears every time that the user performs a password-protected operation.

- c. In the **Password check** 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 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, click the **Save** button.

Managing Kaspersky Security settings

This section contains instructions on transferring configured Kaspersky Security settings to an application installed on a different virtual machine and restoring the standard application settings.

In this section:

Importing Kaspersky Security settings into an application installed on another virtual machine	258
Restoring the default application settings	260

Importing Kaspersky Security settings into an application installed on another virtual machine

After configuring Kaspersky Security settings, you can apply the same settings to the application installed on a different virtual machine. As a result, Kaspersky Security will be configured identically on both virtual machines.

You can save application settings in a special configuration file in CFG format and then export the configuration file from one virtual machine to another.

The configuration file in CFG format is also used to import settings during remote installation of the application and during the process of creating a Light Agent policy (for details see the *Administrator's Guide for Kaspersky Security for Virtualization 4.0 Light Agent*). The configuration file used to import settings during remote installation of the application must have the following name: `install.cfg`.

► *To transfer Kaspersky Security settings to the application installed on another virtual machine:*

1. Save the current Kaspersky Security to a configuration file as follows:

a. Open the application settings window (see page [25](#)).

b. In the left part of the window, select the **Advanced Settings** section.

Advanced application settings are displayed in the right part of the window.

c. In the **Manage settings** section, click the **Save** button.

A standard Microsoft Windows **Please select a configuration file** window opens.

d. Enter the name of the configuration file and the path where it should be saved.

e. Click the **Save** button.

2. Move the configuration file you have saved to another virtual machine (for example, send it by email or use a removable drive).

3. On the other virtual machine, import the settings into Kaspersky Security from the configuration file as follows:

a. Open the application settings window.

b. In the left part of the window, select the **Advanced Settings** section.

Advanced application settings are displayed in the right part of the window.

c. In the **Manage settings** section, click the **Load** button.

A standard Microsoft Windows **Please select a configuration file** window opens.

d. Select the file from which you wish to import the Kaspersky Security settings.

e. Click the **Open** button.

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

Restoring the default application settings

Based on the information about the operating system and applications installed on the protected virtual machine, Kaspersky Lab specialists will recommend optimum security settings for the virtual machine. While using Kaspersky Security, you can always restore the standard application settings. The settings can be restored using the Initial Configuration Wizard.

► *To restore the standard application settings:*

1. Open the application settings window.
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. In the **Manage settings** section, click the **Restore** button.

The Initial Configuration Wizard starts.

4. In the **General information** window, click the **Next** button to start using the Initial Configuration Wizard.
5. The **Restore settings** window shows the Kaspersky Security components and tasks whose settings have been modified.

If custom settings have been created for any of the components during the operation of any component, they are also shown in this window. Special settings include lists of trusted web addresses, exclusions, Firewall network rules, Application Control rules, and others.

Custom settings are created as you use Kaspersky Security, taking into account your individual tasks and security needs. Custom settings normally take a lot of time to create, which is why Kaspersky Lab specialists recommend saving them. Otherwise, all settings created during operation of the application will be lost.

Select check boxes opposite the components and tasks for you which you want to restore the standard settings.

6. Click the **Next** button.
7. At the next stage, the Initial Configuration Wizard analyzes information about Microsoft Windows applications. These applications end up in the list of trusted applications (see section "Creating the list of trusted applications" on page [225](#)) that are not subject to restrictions applicable to operations performed in the operating system. The data analysis process is displayed in the **System analysis** window.

After completing analysis of the operating system, the Initial Configuration Wizard automatically proceeds to the next step.

8. In the **Finishing the initial configuration of application** window, click **Finish**.

The Initial Configuration Wizard closes, and the standard application settings are restored.

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

Participating in Kaspersky Security Network

This section covers participation in Kaspersky Security Network and provides instructions on how to check the connection to Kaspersky Security Network.

In this section:

About participation in Kaspersky Security Network.....	262
Checking the connection to Kaspersky Security Network.....	263

About participation in Kaspersky Security Network

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

Kaspersky Security Network (KSN) is an infrastructure of cloud services providing access to Kaspersky Lab's online knowledge base with information about the reputation of files, web resources, and software. Using data from Kaspersky Security Network ensures a faster response time for Kaspersky Security when encountering new types of threats and improves performance of some protection components.

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.

The following types are differentiated depending on the location of the infrastructure:

- Global KSN – this infrastructure is hosted by Kaspersky Lab servers.
- Private KSN (Kaspersky Private Security Network) – the infrastructure is hosted by third-party servers of the service provider, for example on the Internet service provider's network.

Usage of Private KSN can be configured in the properties of the Administration Server of Kaspersky Security Center in the **KSN proxy server** section. See Kaspersky Security Center documentation for more information.

To continue using Private KSN after the key has been changed, send information about the new key to the service provider. Otherwise, data exchange with KSN will not be possible.

While using KSN, the application automatically sends to Kaspersky Security Network the statistics generated during its operation (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*). Kaspersky Lab protects any information received in this way as prescribed by law and applicable rules of Kaspersky Lab.

Kaspersky Lab uses any received information in anonymized form and as general statistics only. General statistics are automatically generated using original collected information and do not contain any personal or other confidential data. The original information received is destroyed as new information is accumulated (once a year). General statistics are stored indefinitely. More information about submission of statistical information generated during participation in Kaspersky Security Network, storage and destruction of such information is available in the KSN Statement and on the Kaspersky Lab website at <http://www.kaspersky.com/privacy>.

Participation in Kaspersky Security Network is voluntary. The usage of KSN can be enabled or disabled by the application administrator in policy settings (see the *Administrator's Guide to Kaspersky Security for Virtualization 4.0 Light Agent*).

Checking the connection to Kaspersky Security Network

► *To check the connection to Kaspersky Security Network:*

1. Open the main application window (see page [23](#)).
2. In the upper part of the window, click the **Kaspersky Security Network** button.

The **Kaspersky Security Network** window opens.

The round **KSN** button in the left part of the window reflects the mode of application connection to Kaspersky Security Network:

- If Kaspersky Security is connected to Kaspersky Security Network, the **KSN** button is green. The following information appears under the **KSN** button: *Enabled* status, type of KSN in use: Private KSN (KPSN) or Global KSN, and the time of the last synchronization with KSN servers. File and web resource reputation statistics are shown in the right part of the window.

Kaspersky Security receives statistical data on the usage of Kaspersky Security Network services when you open the **Kaspersky Security Network** window. The statistics are not updated in real time.

- If Kaspersky Security is not connected to Kaspersky Security Network, 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 application has not been activated or the license has expired.
- You are not a participant in Kaspersky Security Network.
- The KSN Proxy service is disabled in Kaspersky Security Center (see Kaspersky Security Center manuals).

Glossary

A

Application databases

Databases that contain descriptions of computer security threats that are known to Kaspersky Lab by the moment of release of the databases. Application databases are compiled by Kaspersky Lab specialists and are updated hourly.

Archive

One or several file(s) packaged into a single file through compression. A dedicated application, called an archiver, is required for packing and unpacking data.

Autorun objects

A set of applications needed for the operating system and software that is installed on the virtual machine to start and operate correctly. The operating system launches these objects at every startup. There are viruses capable of infecting such objects specifically, which may lead, for example, to blocking of operating system startup.

B

Backup

A dedicated storage for backup copies of files that have been deleted or modified during disinfection.

Backup copy of a file

A copy of a virtual machine file that is created when this file is disinfected or removed. Backup copies of files are stored in Backup in a special format and pose no danger.

C

Compound file

A compound file is comprised of several individual files that are stored in one physical file, and each of those files is accessible. Examples of compound files include archives, installation packages, embedded OLE objects, and files in email formats. A common technique for concealing viruses is to implant them into compound files. To detect viruses concealed using this method, the compound file must be unpacked.

D

Database of malicious web addresses

A list of addresses of web resources 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.

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.

F

False positive

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.

H

Heuristic Analysis

A technology for detecting threats information about which has not yet been added to Kaspersky Lab application databases. It detects files that may be infected with malware for which there are no database signatures yet or with a new variety of a known virus.

I

Infected object

It is the object, which contains a part of code that matches completely a part of code of a well-known harmful application. Kaspersky Lab does not recommend using such objects.

K

Kaspersky Private Security Network

A solution that allows users of Kaspersky Lab anti-virus applications to access Kaspersky Security Network databases without sending data from their computers to Kaspersky Security Network servers.

Kaspersky Security Network (KSN)

An infrastructure of cloud services that provides access to the online Knowledge Base of Kaspersky Lab which contains information about the reputation of files, web resources, and software. The use of data from Kaspersky Security Network ensures faster responses by Kaspersky Lab applications to threats, improves the performance of some protection components, and reduces the likelihood of false alarms.

Keylogger

A program designed for hidden logging of information about keys pressed by the user. Keyloggers function as keystroke interceptors.

O

OLE object

An object attached to another file or embedded into another file through the use of the Object Linking and Embedding (OLE) technology. An example of an OLE object is a Microsoft Office Excel® spreadsheet embedded into a Microsoft Office Word document.

P

Phishing

A kind of online fraud aimed at obtaining unauthorized access to confidential data of users.

Protected virtual machine

A virtual machine with the Light Agent component installed.

S

Signature Analysis

A threat detection technology which uses the Kaspersky Lab application databases that contain descriptions of known threats and methods for neutralizing them. Protection that uses signature analysis provides the minimum acceptable security level. As recommended by Kaspersky Lab experts, the application always has this analysis method enabled.

SVM

Secure virtual machine, SVM. A virtual machine deployed on a hypervisor with the Protection Server component of Kaspersky Security installed.

AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against various threats, including viruses and other malware, unsolicited email (spam), network and hacking attacks.

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 vendor of computer protection systems for home users in Russia ("IDC Endpoint Tracker 2014").

Kaspersky Lab was founded in Russia in 1997. Today, Kaspersky Lab is an international group of companies running 34 offices in 31 countries. The company employs more than 3000 qualified specialists.

Products. Kaspersky Lab's products provide protection for all systems – from home computers to large corporate networks.

The personal product range includes applications that provide information security for desktop, laptop, and tablet computers, as well as for smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with Kaspersky Lab's centralized management tools, these solutions ensure effective automated protection against computer threats for organizations of any scale. 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 thousands of new computer threats, create tools to detect and disinfect them, and include them in the databases used by Kaspersky Lab applications.

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 software developers use the Kaspersky Anti-Virus kernel in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. 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. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was eventually awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab's website: <http://www.kaspersky.com>

Virus Encyclopedia: <https://securelist.com/>

Virus Lab: <http://newvirus.kaspersky.com> (for analyzing suspicious files and websites)

Kaspersky Lab's web forum: <http://forum.kaspersky.com/index.php?s=51326149e615749dc3cf141fc800dfe0&showforum=3>

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.

Adobe and Acrobat are the trademarks or registered trademarks of Adobe Systems Incorporated in the United States and / or elsewhere.

Citrix and XenServer are trademarks of Citrix Systems, Inc. and / or subsidiaries, registered with the US Patent Office and the patent offices of other countries.

FireWire is a trademark of Apple Inc., registered in the USA and elsewhere.

ICQ is a trademark and / or service mark of ICQ LLC.

Microsoft, Excel, Hyper-V, Outlook, Windows and Windows Server are trademarks of Microsoft Corporation, registered in the USA and elsewhere.

Mozilla and Thunderbird are trademarks of Mozilla Foundation.

VMware ESXi is a trademark of VMware, Inc., or trademark of VMware, Inc. registered in the USA or in other jurisdictions.

The wordmark Bluetooth and its logo are the property of Bluetooth SIG, Inc.

Index

A

Access rules

access to devices	159
access to web resources	174

Actions to perform on objects	42, 55, 67, 194
-------------------------------------	-----------------

Application components	17
------------------------------	----

Application databases	212
-----------------------------	-----

Application group network rules	91
---------------------------------------	----

Application icon	21
------------------------	----

Application network rules	100
---------------------------------	-----

Application Privilege Control	138
-------------------------------------	-----

application control rules	144
---------------------------------	-----

enabling and disabling	139
------------------------------	-----

Application Self-Defense	251
--------------------------------	-----

Application settings window	25
-----------------------------------	----

Application Startup Control	124
-----------------------------------	-----

Application Startup Control rules	127
---	-----

enabling and disabling	125
------------------------------	-----

operating modes	129
-----------------------	-----

B

Backup	228, 231
--------------	----------

- configuring settings 229
- Deleting an object..... 233
- restoring an object..... 232

C

Control rules

- application startup 127
- applications 144

D

- Device Control 157
- devices access rules 159

E

- Exclusions..... 217

F

- File Anti-Virus 36
- enabling and disabling..... 37
- Heuristic Analysis 45
- optimization of scanning 47
- protection scope 43
- scanning compound files 47
- security level 41
- Firewall 79

H

Heuristic Analysis

File Anti-Virus	45
IM Anti-Virus.....	77
Mail Anti-Virus	60
Web Anti-Virus	69

I

IM Anti-Virus

enabling and disabling.....	73
Heuristic Analysis	77
protection scope	75

K

Kaspersky Security Network	262
----------------------------------	-----

M

Main application window	23
-------------------------------	----

N

Network connection status	83
Network Monitor.....	117
Network packet rules	84
Network rules.....	82
Notifications	243

P

Protection scope	
File Anti-Virus	43
IM Anti-Virus.....	75
Mail Anti-Virus	56
Protection status	29

R

Reports	234
configuring settings	236
exporting to file	239
generating	238
viewing	238
Restoring the default settings.....	260
Restricting access to the application	254

S

Scan	
optimization of scanning	47, 199
run mode	203
scan scope	195
scan technology	46, 202
scanning compound files	47, 200
scanning removable drives	206
starting the task	190

tasks.....	189
Scan scope.....	195
Scanning virtual machines	189
System Watcher.....	119

T

Task.....	17, 189
custom scan.....	189
full scan.....	189
Trusted applications.....	219, 225
Trusted devices	159
Trusted zone.....	217

U

Update	17, 212
Updates	
manual launch.....	213
update task.....	213

W

Web Anti-Virus	
enabling and disabling.....	63
Heuristic Analysis	69
security level	66
Web Control.....	171